21世纪高职高专规划教材

计算机应用系列

计算机网络管理与安全

（第2版）

赵立群　主编

吴　霞　孙　岩　副主编



清华大学出版社

21 世纪高职高专规划教材·计算机应用系列

计算机网络管理与安全
（第 2 版）

赵立群　主　编
吴　霞　孙　岩　副主编

清 华 大 学 出 版 社
北　京

内 容 简 介

本书主要讲解计算机网络管理技术和安全技术两部分内容。在网络管理技术中重点介绍基于SNMP的网络设备管理技术、基于Windows的活动目录技术、局域网监控技术;在网络安全方面,侧重介绍网络信息安全和系统安全,并结合实例说明与操作演示指导学生实训、加强实践,强化技能培养。

由于本书融入计算机网络管理与安全最新的实践教学理念,力求严谨、注重与时俱进,具有知识系统、语言简洁、突出实用性等特点,并注重职业技术与实践应用相结合。本书既可作为高职高专院校计算机应用和网络管理等专业的教材,也可作为企业信息化培训教材,还可作为广大企事业网站建设从业及管理者自学参考读物。

图书在版编目(CIP)数据

计算机网络管理与安全/赵立群主编.--2版.--北京:清华大学出版社,2014
21世纪高职高专规划教材.计算机应用系列
ISBN 978-7-302-37606-4

Ⅰ.①计… Ⅱ.①赵… Ⅲ.①计算机网络－管理－高等职业教育－教材 ②计算机网络－安全技术－高等职业教育－教材 Ⅳ.①TP393

中国版本图书馆CIP数据核字(2014)第186513号

责任编辑:田 梅
封面设计:傅瑞学
责任校对:刘 静
责任印制:

出版发行:清华大学出版社
网 址:http://www.tup.com.cn,http://www.wqbook.com
地 址:北京清华大学学研大厦A座 **邮 编**:100084
社 总 机:010-62770175 **邮 购**:010-62786544
投稿与读者服务:010-62776969,c-service@tup.tsinghua.edu.cn
质量反馈:010-62772015,zhiliang@tup.tsinghua.edu.cn
课件下载:http://www.tup.com.cn,010-62795764
印 刷 者:
装 订 者:
经 销:全国新华书店
开 本:185mm×260mm **印 张**:16 **字 数**:366千字
版 次:2008年10月第1版 2014年12月第2版 **印 次**:2014年12月第1次印刷
印 数:1～
定 价: .00元

产品编号:061218-01

编　委　会

序言

随着微电子技术、计算机技术、网络技术、通信技术、多媒体技术等高新科技日新月异的飞速发展和普及应用，不仅有力地促进了各国经济发展、加速了全球经济一体化的进程，而且推动着当今世界跨入信息社会的步伐。以计算机为主导的计算机文化，正在深刻地影响着人类社会的经济发展与文明建设，以网络为基础的网络经济，正在全面地改变着传统的社会生活、工作方式和商务模式。如今，计算机应用水平、信息化发展速度与程度，已经成为衡量一个国家经济发展和竞争力的重要指标。

没有计算机就没有现代化发展！没有计算机网络，就没有经济的大发展！为此，国家出台了一系列“关于加强计算机应用和推动国民经济信息化进程的文件及规定”，启动了“电子商务、电子政务、金税”等富有深刻意义的重大工程，加速推进“国防信息化、金融信息化、财税信息化、企业信息化、教育信息化、社会管理信息化”，因而全社会又掀起了新一轮的计算机学习应用的热潮。

针对我国高职教育“计算机应用”等专业知识老化、教材陈旧、重理论轻实践、缺乏实际操作技能训练的问题，为了适应我国国民经济信息化发展对计算机应用人才的需要，全面贯彻教育部关于“加强职业教育”的精神和“强化实践实训、突出技能培养”的要求，根据企业用人与就业岗位的真实需要，结合高职高专院校“计算机应用”和“网络安全”等专业的教学计划及课程设置与调整的实际情况，我们组织北京联合大学、陕西理工学院、北方工业大学、沈阳师范大学、北京财贸职业学院、山东滨州职业学院、首钢工学院、包头职业技术学院、北方工业技术学院、广东理工学院、北京城市学院、黑龙江工商大学、北京石景山社区学院、海南职业学院、北京西城经济科学大学、北京朝阳社区学院、北京宣武社区学院等全国30多所高校及高职院校多年从事计算机教学的主讲教师和具有丰富实践经验的企业人士共同撰写了此套教材。

本套教材包括《计算机基础实例教程》、《中小企业网站建设与管理》等16本书。在编写过程中，编者们注意自觉坚持以科学发展观为统领，严守统一的创新型格式化设计；注重校企结合、贴近行业企业岗位实际，注重实用技术与能力的训练培养，注重实践技能应用与工作背景紧密结合，同时也注重计算机、网络、通信、多媒体等现代化信息技术的新发展，具有集成性、系统性、针对性、实用性、易于实施教学等特点。

本套教材不仅适合高职高专及应用型院校"计算机应用、网络、电子商务"等专业学生的学历教育，同时也可作为工商、外贸、流通等企事业单位从业人员的职业教育和在职培训，对于广大社会自学者也是有益的学习参考读物。

系列教材编委会

2014年5月

第 2 版前言

计算机网络管理与安全既是信息化推进的基础保障，也是信息系统正常运行的关键环节。管理信息系统是企事业单位计算机应用的灵魂，而网络系统安全则是管理信息系统最重要的安全防护保障支撑；并在国家机密安全防护、有效保护企业商业秘密和公民个人隐私等方面发挥越来越重要的作用。

"计算机网络管理与安全"是计算机网络管理专业非常重要的专业课程，也是学生就业、从事相关工作必须掌握的关键知识技能。本书注重以学习者应用能力培养和提高为主线、坚持以科学发展观为统领，严格按照教育部关于"加强职业教育、突出实践技能培养"的要求，根据计算机网络管理与安全技术设备的发展、结合高职高专教学改革的需要，针对知识要点、难点循序渐进地进行讲解。

本书自出版以来，因写作质量高而深受全国各类高校广大师生的欢迎，目前已多次重印。此次再版，结合读者对本教材提出的意见和建议，作者审慎地对原教材进行了反复推敲和认真完善的修订，在保留原书特点和基本结构的基础上，进行知识更新、软件更新，增加新知识、补充操作实训，以便更好地为计算机应用教学实践服务。

本书作为高职高专计算机网络管理专业的特色教材，按照计算机网络安全管理的基本过程和规律，主要对计算机网络管理技术和安全技术两部分内容进行介绍。在网络管理技术中重点介绍基于 SNMP 的网络设备管理技术、基于 Windows 的活动目录技术、局域网监控技术；在网络安全方面，侧重介绍网络信息安全和系统安全，并通过结合实例说明与操作演示指导学生实训、加强实践，强化技能培养。

由于本书融入计算机网络安全管理最新的实践教学理念，力求严谨、注重与时俱进，具有知识系统、语言简洁、突出实用性等特点，并注重职业技术与实践应用相结合；因此本书既可作为高职高专院校计算机应用和网络管理等专业的首选教材，也可作为企业信息化培训教材，并为广大企事业网站管理从业者提供有益的学习指导。

本教材由李大军进行统筹策划及具体组织，赵立群主编并统改全稿，吴霞、孙岩为副主编，由Cisco公司高级网络培训师马瑞奇审定。作者写作分工如下：牟惟仲（序言），赵立群（第1章、第7章），唐宏维（第2章、第3章），孙岩（第4章），吴霞、关忠（第5章），温志华（第6章），徐军（第8章），王冰（附录）；华燕萍（文字修改和版式整理），李晓新（制作课件）。

在教材编写的过程中，我们参阅了中外有关计算机网络管理与安全的最新书刊和网站资料，并得到计算机行业协会及业界专家教授的具体指导，在此一并致谢。为方便教学，本书配有电子课件，读者可以从清华大学出版社网站（www.tup.com.cn）免费下载使用。因作者水平有限，书中难免存在疏漏和不足，恳请同行批评指正。

编　者

2014年9月



随着计算机技术与网络通信技术的飞速发展，计算机网络应用已经渗透到社会经济领域的各个方面。计算机网络技术是现代信息科学与技术的重要组成部分，也是计算机管理信息系统的核心；计算机网络管理与安全既是信息化推进的基础保障，也是信息系统正常运行的关键环节，因而备受世界各国高度关注。

本教材针对计算机网络管理与安全等方面存在的管理及技术问题，按照教育部关于"加强职业教育、强化实践教学、突出技能和能力培养"教育教学改革精神，根据计算机网络管理与安全课程教学规律和特点，对原有的计算机网络管理、网络安全等内容进行了深度综合与提炼，并注意打通相关知识联系，采取了集成式写法。本书内容包括：基于Windows操作系统的活动目录管理方法、网络操作系统、网络管理、对因特网工作环境的支持、网络安全技术与应用、SNMP协议管理等基本知识，以及加强计算机网络安全管理等技术应用。

全书共8章，采取新颖统一的格式化设计，突出案例教学，在案例的选择上具有实用性，以学习者应用能力培养与提高为主线，依照学习计算机网络管理与安全的基本过程和规律，以任务剖析的方式，结合知识要点循序渐进地进行讲解。本书在引导读者对知识和技术理解与掌握的基础上，通过多动手、多练习的方式，提高实践应用技能，注重动手能力的培养，以达到学以致用的目的。

目前，世界正处于科学技术的高速发展期，我国也正处在经济发展最活跃的时期，面对激烈的市场竞争，面对科技进步，所有企事业单位都在科学发展观的统领下加快信息化进程，加速信息技术应用，特别关注和加强计算机网络管理与安全的监控。当前面临企业拼发展，面临社会就业上岗的巨大压力，无论是企业员工、即将毕业的各类学生，还是下岗转岗的待业人员，努力学习和掌握计算机网络管理与安全的软件工具及技术应用，不断提高业务技术素质，对于今后的发展都具有特殊意义。

本教材由李大军进行总体方案策划并具体组织，赵立群主编并统编全稿，车亚军和车东升为副主编，本书由具有丰富专业教学和企业实践经验的杜春涛教授审定。参加编写的人员有：车亚军（第1章），李多（第2章），王海珊（第3章），杨春（第4章），赵立群（第5章），孙钢凝（第6章），关忠（第7章），车东升（第8章）。

本书在编写过程中，广泛征集了各高等职业院校计算机网络管理与安全课程的主讲老师和有关企事业单位计算中心负责人对本书的修改意见与建议，得到了我国有关计算机行业协会的支持与帮助，得到了长期从事计算机教育教学有关专家教授的指导；在此，对参与本书出版论证与写作指导的牟惟仲、王纪平、张昌连、冀俊杰、吴明、林亚、储祥银、丁建忠、侯杰、沈煜、赵茜等同志一并表示衷心地感谢。由于时间紧，在编写过程中难免存在不足和疏漏，恳请各位专家及读者给予批评指正。

编　者

2007 年 7 月

目录

第1章

网络管理概述

【本章重点】

计算机网络管理的概念、功能，网络管理软件的分类。SNMP 的作用和基本内容，Windows 的活动目录和组策略技术，局域网监控软件的作用和其中的主要技术。

计算机网络作为计算机技术和通信技术相结合的产物，近年来得到了迅猛的发展。随着规模的不断扩大，网络中的设备越来越多、异构性越来越强。同时随着计算机网络越来越快地进入我们的工作与生活，人们对计算机网络的依赖性越来越高。

这就使得计算机网络运行的可靠性、安全性变得至关重要，向网络的管理、运行提出了更高的要求；网络系统的维护与管理日趋繁杂，网络管理人员用人工方法管理网络已无法可靠、迅速地保障网络的正常运行，甚至无法满足当前开放式异构网络环境的需要；人们迫切地需要用计算机来管理网络，提高网络管理水平，使计算机网络能够安全、快捷地传递用户所需要的信息。于是计算机网络管理理论便应运而生了。

1.1 网络管理

作为一种正在发展中的技术，无论是从理论还是从实践出发，对于网络管理都必须有一个确定的概念，同时对网络管理的对象有一个较为明确的界定。

1.1.1 计算机网络管理概念

所谓计算机网络管理就是指规划、监督、设计和控制网络资源的使用和网络的各种活动，以使网络的性能达到最优。通俗地讲，网络管理就是通过某种方式对网络状态进行调整，使网络能正常、高效地运行，使网络中各种资源得到更加高效的利用，当网络出现故障时能及时做出报告和处理，并协调、保持网络的高效运行等。

一般来说，从网络管理概念的范畴来分类，可分为对网“路”的管理，即针对交换机、路由器等主干网络进行管理；对接入设备的管理，即对内部 PC、服务器、交换机等进行管理；对行为的管理，即针对用户的使用进行管理；对资产的管理，即统计 IT 软硬件的信息等。计算机网络管理具有 5 大功能。

1. 故障管理

故障管理(Fault Management)是网络管理中最基本的功能之一。用户都希望有一个可靠的计算机网络。当网络中某个组成失效时,网络管理器必须迅速查找到故障并及时排除。通常不大可能迅速隔离某个故障,因为网络故障的产生原因往往相当复杂,特别是当故障是由多个网络组成共同引起时。在此情况下,一般先将网络修复,然后再分析网络故障的原因。分析故障原因对于防止类似故障的再发生相当重要。

2. 计费管理

计费管理(Accounting Management)记录网络资源的使用,目的是控制和监测网络操作的费用和代价。它对一些公共商业网络尤为重要。它可以估算出用户使用网络资源可能需要的费用和代价,及已经使用的资源。网络管理员还可规定用户可使用的最大费用,从而控制用户过多占用和使用网络资源。这也从另一方面提高了网络的效率。另外,当用户为了一个通信目的需要使用多个网络中的资源时,计费管理应可以计算总计费用。

3. 配置管理

配置管理(Configuration Management)同样相当重要。它初始化网络并配置网络,以使其提供网络服务。配置管理是一组对辨别、定义、控制和监视组成一个通信网络的对象所必要的相关功能,目的是为了实现某个特定功能或使网络性能达到最优。

(1) 配置信息的自动获取

在一个大型网络中,需要管理的设备是比较多的,如果每个设备的配置信息都完全依靠管理人员的手工输入,工作量是相当大的,而且还存在出错的可能性。对于不熟悉网络结构的人员来说,这项工作甚至无法完成。因此一个先进的网络管理系统应该具有自动获取配置信息功能。即使在管理人员不是很熟悉网络结构和配置状况的情况下,也能通过有关的技术手段来完成对网络的配置和管理。

在网络设备的配置信息中,根据获取手段可以分为三类:第一类是网络管理协议标准的 MIB 中定义的配置信息(包括 SNMP 和 CMIP);第二类是不在网络管理协议标准中有定义,但是对设备运行比较重要的配置信息;第三类就是用于管理的一些辅助信息。

(2) 自动配置、自动备份及相关技术

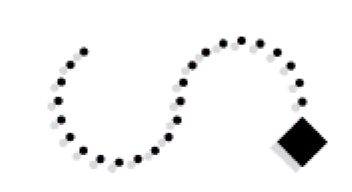
配置信息自动获取功能相当于从网络设备中“读”信息,在网络管理应用中还有大量“写”信息的需求。同样根据设置手段对网络配置信息进行分类:第一类是可以通过网络管理协议标准中定义的方法(如 SNMP 中的 set 服务)进行设置的配置信息;第二类是可以通过自动登录到设备进行配置的信息;第三类就是需要修改的管理性配置信息。

(3) 配置一致性检查

在一个大型网络中,由于网络设备众多,而且由于管理的原因,这些设备很可能不是由同一个管理人员进行配置的。因此,对整个网络的配置情况进行一致性检查是必需的。在网络的配置中,对网络正常运行影响最大的主要是路由器端口配置和路由信息配置,因此,要进行一致性检查的也主要是这两类信息。

(4) 用户操作记录功能

配置系统的安全性是整个网络管理系统安全的核心,因此,必须对用户进行的每一配



置操作进行记录。在配置管理中，需要对用户操作进行记录，并保存下来。管理人员可以随时查看特定用户在特定时间内进行的特定配置操作。

4. 性能管理

性能管理(Performance Management)主要针对系统资源的运行状况及通信效率等系统性能，其能力包括监视和分析被管网络及其所提供服务的性能机制。性能分析的结果可能会触发某个诊断测试过程或重新配置网络以维持网络的性能。性能管理收集分析有关被管网络当前状况的数据信息，并维持和分析性能日志，一些典型的功能如下。

(1) 性能监控：由用户定义被管对象及其属性。被管对象类型包括线路和路由器；被管对象属性包括流量、延时、丢包率、CPU 利用率、温度、内存余量。对于每个被管对象，定时采集性能数据，自动生成性能报告。

(2) 阈值控制：可对每一个被管对象的每一条属性设置阈值，对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进行阈值设置。可通过设置阈值检查开关控制阈值检查和告警，提供相应的阈值管理和溢出告警机制。

(3) 性能分析：对历史数据进行分析、统计和整理，计算性能指标，对性能状况做出判断，为网络规划提供参考。

(4) 可视化的性能报告：对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果。

(5) 实时性能监控：提供了一系列实时数据采集；分析和可视化工具，用于对流量、负载、丢包、温度、内存、延时等网络设备和线路的性能指标进行实时检测，可任意设置数据采集间隔。

(6) 网络对象性能查询：可通过列表或按关键字检索被管网络对象及其属性的性能记录。

5. 安全管理

安全性一直是网络的薄弱环节之一，而用户对网络安全的要求又相当高，因此网络安全管理(Security Management)非常重要。网络中主要有几大安全问题：网络数据的私有性(保护网络数据不被侵入者非法获取)，授权(authentication，防止侵入者在网络上发送错误信息)，访问控制(控制对网络资源的访问)。

相应地，网络安全管理应包括对授权机制、访问控制、加密和加密关键字的管理，另外还要维护和检查安全日志，包括网络管理过程中，存储和传输的管理和控制信息对网络的运行和管理至关重要，一旦泄密、被篡改或伪造，将给网络造成灾难性的破坏。

1.1.2 网络管理软件

1. 网络管理软件的分类

常用的网络管理软件可分为两大类，主要根据管理对象来分，即通用网络管理软件(NMS)和网元(设备)管理软件(EMS)两大类，网元管理软件只管理单独的网元(网络设备)，通用网络管理软件的管理目标为一个网络。

网元管理软件一般由原厂商提供，各厂商采用专有的管理 MIB 库，以实现对厂商设

备本身的细致入微的管理，包括可以显示出厂商设备图形化的面板等，如安奈特公司的AT-View Plus，思科公司的Cisco View和华为网络公司的Quidview等。

通用网络管理软件则主要用于掌握全网的状况，作为底层的网管平台来服务于上层的网元管理软件等，可以提供一个第三方的网管平台，支持对所有SNMP设备的发现和监控，可集成厂商设备的私有MIB库，可实现对全网（多厂商）设备进行识别和统一的管理，从而避免了厂商专用型网管软件无法实现对全网设备的统一管理，用户往往采用多台网管工作站分别安装不同的系统进行分别管理，有利于简化管理和降低成本。这类产品还有惠普公司的HP OpenView、CA公司的Unicenter、IBM公司的Tivoli NetView等。

本书重点介绍通过网络管理系统对网络进行有效的管理。

2. 网络管理系统的主要功能

网管系统开发商针对不同的管理内容开发了相应的管理软件，形成了多个网络管理方面。目前主要的几个发展方面有：网管系统（NMS）、应用性能管理（APM）、应用性能管理、桌面管理（DMI）、员工行为管理（EAM）、安全管理。当然传统网络管理模型中的资产管理、故障管理仍然是热门的管理课题。

（1）网管系统（NMS）。

网管系统主要是针对网络设备进行监测、配置和故障诊断的，主要功能有自动拓扑发现、远程配置、性能参数监测、故障诊断。网管系统主要由两类公司开发，一类是通用软件供应商；另一类是各个设备厂商。

通用软件供应商开发的NMS系统是针对各个厂商网络设备的通用网管系统，目前比较流行的有OpenView、Micromuse、Concord等。

各个设备厂商为自己产品设计的专用NMS系统对自己产品的监测、配置功能非常全面，可监测一些通用网管系统无法监测的重要性能指标，还有一些独特的配置功能。但是对其他公司生产的设备基本上就无能为力了。目前比较流行的设备厂商网管软件有Cisco Works 2000、NetSight，国内的Linkmanage、iManager。

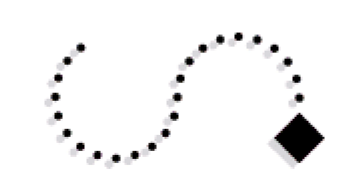
（2）应用性能管理（APM）。

应用性能管理是一个比较新的网络管理方向，主要指对企业的关键业务应用进行监测、优化，提高企业应用的可靠性和质量，保证用户得到良好的服务，降低IT总拥有成本（TCO）。一个企业的关键业务应用性能的强大，可以提高竞争力，并取得商业成功，因此，加强应用性能管理（APM）可以产生巨大的商业利益。应用性能管理主要功能如下。

监测企业关键应用性能：过去，企业的IT部门在测量系统性能时，一般重点测量为最终用户提供服务的硬件组件的利用率，如CPU利用率以及通过网络传输的字节数。虽然这种方法也提供了一些宝贵的信息，但却忽视了最重要的因素——最终用户的响应时间。现在通过事务处理过程监测、模拟等手段可真实测量用户响应时间，此外还可以报告谁正在使用某一应用、该应用的使用频率以及用户所进行的事务处理过程是否成功完成。

快速定位应用系统性能故障：通过对应用系统各种组件（数据库、中间件）的监测，迅速定位系统故障，如发生Oracle数据库死锁等问题。

优化系统性能：精确分析系统各个组件占用系统资源情况，中间件、数据库执行效



率，根据应用系统性能要求提出专家建议，保证应用在整个寿命周期内使用的系统资源最少，节约 TCO。

目前市场上比较流行的应用性能管理产品有 BMC、Tivoli Application Performance Management、VERITAS(precise)的 i3 系列产品，Quest 系列产品，Topaz。国内主要是 SiteView 产品。

(3)桌面管理系统(DMI)。

桌面管理环境是由最终用户的计算机组成的，这些计算机运行 Windows、Mac 等系统。桌面管理是对计算机及其组件进行管理，内容比较多，目前主要关注资产管理、软件派送和远程控制。桌面管理系统通过以上功能，一方面减少了网管人员的劳动强度；另一方面增加了系统维护的准确性、及时性。这类系统通常分为两部分——管理端和客户端。

目前市场上比较流行的国外桌面管理系统有 CA Unicenter、Landesk，国内的 NetInhandLANDesk Management Suite 7 是目前比较流行的桌面管理系统。

(4) 员工行为管理(EAM)。

员工行为管理包括两部分，一部分是员工网上行为管理(EIM)；另一部分是员工桌面行为监测。它一般在 Internet 应用层、网络层对信息控制，对数据根据 EIM 数据库进行过滤；定制因特网访问策略，根据用户、团组、部门、工作站或网络设置不同的因特网访问策略。专门的报表工具有：Websense EIM Reporting Tools 等。

(5) 安全管理。

网络安全管理指保障合法用户对资源安全访问，防止并杜绝黑客蓄意攻击和破坏。它包括授权设施、访问控制、加密及密钥管理、认证和安全日志记录等功能。目前市场上的防火墙产品和 IDS 产品很多，防火墙有 Check Point、NetScreem、Cisco PIX 等。IDS 有 ISS 公司的 RealSecure、Axent 的 ITA、ESM，以及 NAI 的 CyberCopMonitor 等。

1.2　网络设备管理的主要协议

网络是由路由器、交换机、服务器等设备组成的，要确保所有的设备正常运行且处于最佳状态确实是一件非常困难的事情。因为通常情况下这些设备都在离你较远地方。它们不会像你的用户那样，当有一个应用程序问题发生时就打电话通知你。为了解决这个问题，设备生产厂商们在设备中设立了网络管理的功能，使网络管理员可以远程控制这些网络设备并查询它们的状态。

1.2.1　SNMP

简单网络管理协议(SNMP)是最早提出的网络管理协议之一，它得到了业界网络设备生产厂商的广泛支持，其中包括 IBM、HP、Sun 等大厂商。目前 SNMP 已成为网络管理领域中事实上的工业标准，并被广泛支持和应用，大多数网络管理系统和平台都是基于 SNMP 的。

简单网络管理协议(SNMP)在体系结构上分为被管理的设备(Managed Device)、

SNMP 管理器(SNMP Manager)和 SNMP 代理(SNMP Agent)三个部分。被管理的设备是网络中的一个节点,有时被称为网络单元(Network Elements),被管理的设备可以是路由器、网管服务器、交换机、网桥、集线器等。每一个支持 SNMP 的网络设备中都运行着一个 SNMP 代理,它负责随时收集和存储管理信息,记录网络设备的各种情况,网络管理软件再通过 SNMP 通信协议查询或修改代理所记录的信息。

SNMP 代理是驻留在被管理设备上的网络管理软件模块,它收集本地计算机的管理信息并将这些信息翻译成兼容 SNMP 的形式。

SNMP 管理器使用网络管理软件通过 SNMP 来进行管理工作。网络管理软件的主要功能之一,就是协助网络管理员完成管理整个网络的工作。网络管理软件要求 SNMP 代理定期收集重要的设备信息,收集到的信息将用于确定独立的网络设备、部分网络或整个网络运行的状态是否正常。SNMP 管理器定期查询 SNMP 代理收集到的有关设备运转状态、配置及性能等的信息。

SNMP 使用面向自陷的轮询方法(Trap-directed Polling)进行网络设备管理。一般情况下,网络管理工作站通过轮询被管理设备中的代理进行信息收集,在控制台上用数字或图形的表示方式显示这些信息,提供对网络设备工作状态和网络通信量的分析和管理功能。当被管理设备出现异常状态时,管理代理通过 SNMP 自陷立即向网络管理工作站发送出错通知。当一个网络设备产生了一个自陷时,网络管理员可以使用网络管理工作站来查询该设备状态,以获得更多的信息。

管理信息数据库(MIB)是由 SNMP 代理维护的一个信息存储库,是一个具有分层特性的信息集合,它可以被网络管理系统控制。MIB 定义了各种数据对象,如图 1-1 所示,网络管理员可以通过直接控制这些数据对象去控制、配置或监控网络设备。

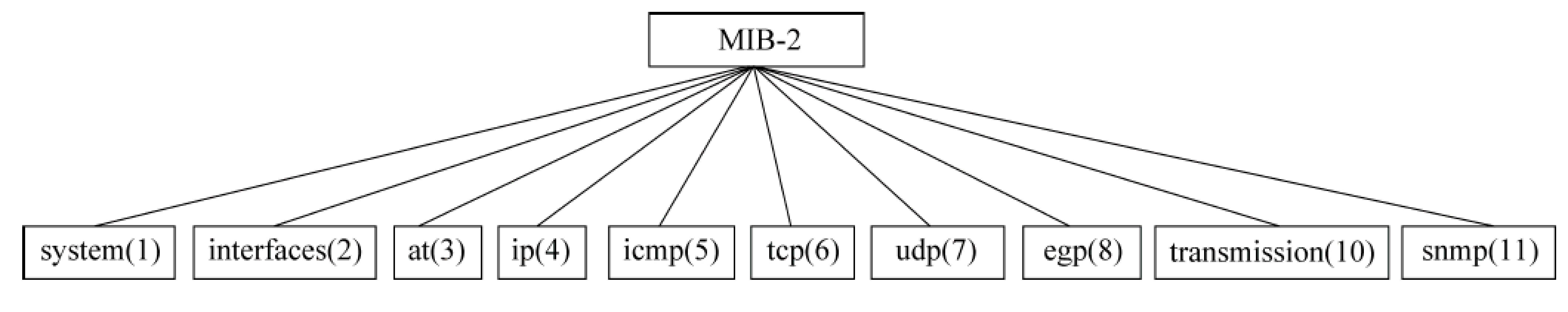
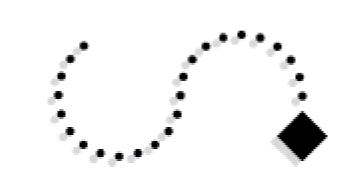


图 1-1　MIB 数据类型

SNMP 通过 SNMP 代理来控制 MIB 数据对象。无论 MIB 数据对象有多少个,SNMP 代理都需要维持它们的一致性,这也是代理的任务之一。现在已经定义的有几种通用的标准管理信息数据库,这些数据库中包括了必须在网络设备中支持的特殊对象,所以这几种 MIB 可以支持简单网络管理协议(SNMP)。使用最广泛、最通用的 MIB 是 MIB-2。此外,为了利用不同的网络组件和技术,还开发了一些其他种类的 MIB。

1.2.2　RMON

远程网络监视(Remote Monitoring On Network,RMON)是 IETF(Internet Engineering Task Force)定义的一种管理信息库(Management Information Base,MIB),



是对 MIB-2 标准最重要的增强。RMON 主要用于对一个网段乃至整个网络中的数据流量的监视，是目前应用相当广泛的网络管理标准之一。

1. 管理信息库

管理信息库(MIB)是被管对象(Router、Bridge、Switch、Hub、网络服务器等设备)的信息集合。标准管理信息库 MIB-2(RFC1213)和各厂家的专有 MIB 库主要提供有关设备的数据，如设备端口状态、流量、错误包数等。网络管理员只能从这些管理信息库中获得单个设备的局部信息。要想获得一个子网网段的信息是非常困难的一件事情，而在规模越来越大的互联网环境中，人们更需要监控的是一个网段的性能，因此仅仅使用标准 MIB 获取设备的管理信息已经不能满足管理大型互联网的要求了。需要以 RMON 解决 SNMP 在日益扩大的分布式互联中所面临的局限性。

RMON 包括 NMS(Network Management Station)和运行在各网络设备上的 Agent 两部分，如图 1-2 所示。RMON Agent 在网络监视器或网络探测器上，跟踪统计其端口所连接的网段上的各种流量信息(如某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等)。

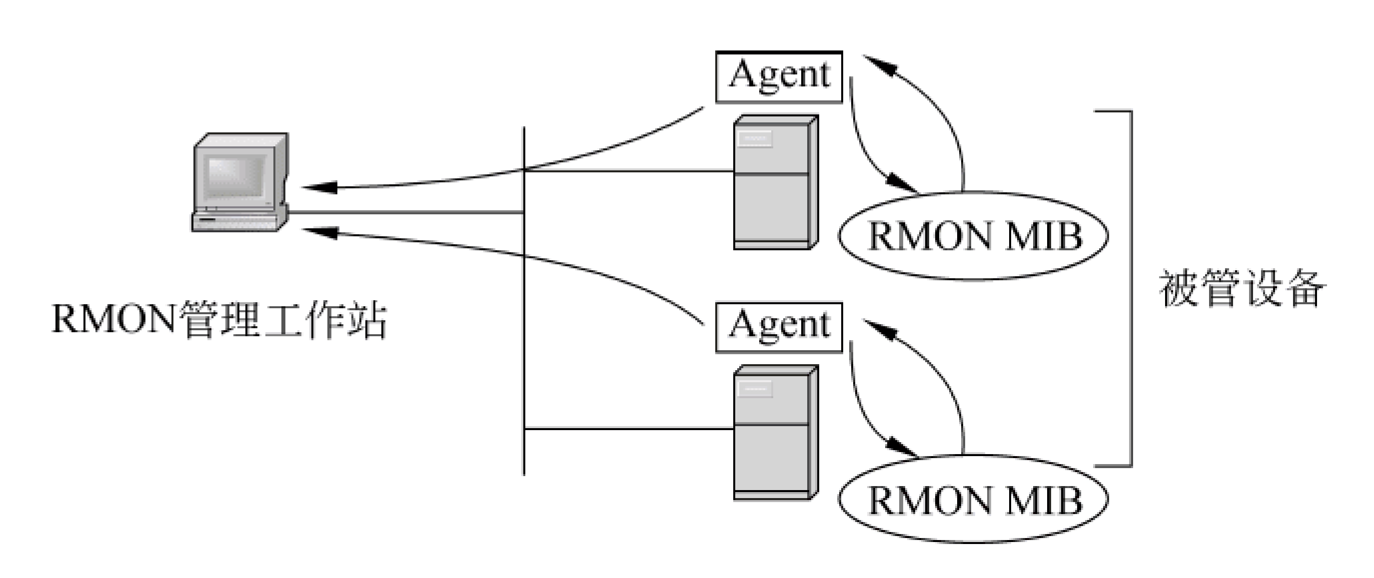


图 1-2　RMON 体系结构

RMON 的实现完全基于 SNMP 体系结构，它与现存的 SNMP 框架兼容，不需要对该协议进行任何修改。RMON 使 SNMP 更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效的手段。RMON 能够减少 NMS 与代理间的通信流量，从而可以简便而有效地管理大型互联网络。

RMON 允许有多个监控者，它可用两种方法收集数据：

第一种方法是利用专用的 RMON Probe(探测仪)收集数据，NMS 直接从 RMON Probe 获取管理信息并控制网络资源。这种方式可以获取 RMON MIB 的全部信息；

第二种方法是将 RMON Agent 直接植入网络设备(路由器、交换机、Hub 等)，使它们成为带 RMON Probe 功能的网络设施。RMON NMS 使用 SNMP 的基本命令与 SNMP Agent 交换数据信息，收集网络管理信息，但这种方式受设备资源限制，一般不能获取 RMON MIB 的所有数据，大多数只收集 4 个组的信息。这 4 个组是告警组、事件组、历史组和统计组。

以太网交换机以第二种方法实现 RMON。以太网交换机里直接植入 RMON Agent，成为带 RMON Probe 功能的网络设施。通过运行在以太网交换机上支持 RMON 的 SNMP Agent，网管站可以获得与以太网交换机端口相连的网段上的整体流量、错误统计和性能统计等信息，实现对网络的管理。

2. 几个常用的 RMON 组

（1）事件组。

事件组用来定义事件号及事件的处理方式。事件组定义的事件主要用在告警组配置项和扩展告警组配置项的告警触发产生的事件中。

事件有以下几种处理方式：将事件记录在日志表中；向网管站发 trap 消息；事件记录在日志表中并向网管站发 trap 消息；不做任何处理。

（2）告警组。

RMON 告警管理可对指定的告警变量（如端口的统计数据）进行监视，当被监视数据的值在相应的方向上越过定义的阈值时会产生告警事件，然后按照事件的定义进行相应的处理。事件的定义在事件组中实现。

用户定义了告警表项后，系统对告警表项的处理如下：对所定义的告警变量（Alarm-Variable）按照定义的时间间隔（Sampling-Time）进行采样；将采样值和设定的阈值进行比较，一旦超过该阈值，即触发相应的事件。

（3）扩展告警。

扩展告警表项可以对告警变量的采样值进行运算，然后将运算结果和设置的阈值比较，实现更为丰富的告警功能。

用户定义了扩展告警表项后，系统对扩展告警表项的处理如下：对定义的扩展告警公式中的告警变量按照定义的时间间隔进行采样；将采样值按照定义的运算公式进行计算；将计算结果与设定的阈值进行比较，一旦超过该阈值，即触发相应事件。

（4）历史组。

配置了 RMON 历史组以后，以太网交换机会周期性地收集网络统计信息，为了便于处理，这些统计信息被暂时存储起来，提供有关网段流量、错误包、广播包、带宽利用率等统计信息的历史数据。

利用历史数据管理功能，可以对设备进行设置。设置的任务包括采集历史数据、定期采集并保存指定端口的数据。

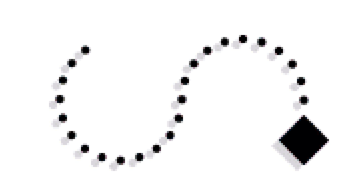
（5）统计组。

统计组信息反映设备上每个监控接口的统计值。统计组统计的是从该统计组创建的时间开始的累计信息。统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。利用 RMON 统计管理功能，可以监视端口的使用情况、统计端口使用中发生的错误。

目前大部分 RMON Agent 只支持统计、历史、告警、事件 4 个组，如 Cisco、3COM、华为的路由器或交换机都已实现了这些功能，对于其他几个组，华为 Qiudway 系列路由器和 LAN Switch 也将会支持。另外，华为 Qiudway 系列路由器增强了 RMON 告警组的功能，不但支持网管站为 Agent 记录的任何计数和整数类对象设置采样间隔和报警阈值，而且允许网管站根据需要以表达式形式对多个变量的组合进行设置。

1.2.3 SMON

早期的网络一般工作在共享模式下，RMON 技术发挥了对共享式网络管理的优势。近年来，随着以交换机设备为主的交换式网络的普遍使用，RMON 技术存在的缺陷逐渐



暴露出来。因此在 RMON 基础上推出了交换机的远程网络监控(Switch Monitoring On Network,SMON)技术标准,随后被 IETF 采纳,在 RFC 2613 文档中进行了详细描述。RMON 和 SMON 的基础是 SNMP,都是通过对 MIB 功能的扩展以适应不断发展的网络技术在管理上的要求。RMON 使 SNMP 适应了共享式网络管理的要求,而 SMON 则为目前广泛使用的交换式网络的管理提供了技术保障。

从实现原理来看,RMON 和 SMON 是对 SNMP 功能的扩展和完善,具体是以扩展 MIB 的结构和功能来实现的。SMON MIB 提供了一个数据结构,列出了进行交换时的数据源和数据源的性能,还增加了那些不适合存放在已有的 RMON 表中的数据源的计数统计能力,SMON MIB 组专门收集物理实体(实体交换机或交换实体模块)和逻辑实体(VLAN)的流量统计和在不同优先级上的流量信息。

在 RMON 中,数据源是 iftable MIB 表中的实体。为了实现 SMON 与 RMON 解决方案之间的兼容,每个新的 SMON 数据源都映射到一个 iftable 实体上,并把这些实体的类型设置为虚拟(virtual)方式。另外,通过使用一个特殊的控制表,可以定义和激活端口复制操作。该表中的每一行都定义了一个激活的端口复制操作,包括将要复制的源端口、目的端口和执行的操作类型(如带内流量复制、带外流量复制,或两者都有)。管理站的管理进程可以通过轮询数据源性能表,发现数据源的端口复制能力。

通过采用这种机制,出现了多端口复制技术,即将多个数据源端口的流量信息同时复制到一个目的端口上,或将一个或多个 VLAN 中的全部流量复制到一个指定的连接端口上。带内流量和带外流量是管理站与 SMON 模块之间的两种工作模式。其中,带内流量方式是指将管理站直接连接到交换机的一个端口上,通过该端口实现与 SMON 模块之间的连接;带外流量方式则是将管理站直接连接到 SMON 模块上,达到直接监控 SMON 的目的。

随着交换技术的不断成熟和完善,出现了三层交换技术,三层交换机也得到了大量应用。三层交换也称多层交换技术或 IP 交换技术,是相对于传统交换概念而提出的。简单地说,三层交换技术就是:二层交换技术+三层转发技术。传统的交换技术是在 OSI 参考模型的第二层(数据链路层)进行操作的,而三层交换技术则在 OSI 参考模型的第三层(网络层)实现了数据包(分组)的高速转发。三层交换技术解决了局域网中网段划分之后,不同网段之间的通信必须依赖路由器进行管理的局面,解决了传统路由器低速、复杂所造成的网络瓶颈问题。

针对三层交换机的应用,IETF 提出了 SMON Ⅱ标准,它可以实现第三层及更高层交换环境的监控。SMON Ⅱ不仅能够对主机的 IP 分组流量独立进行统计,而且能够统计位于其他子网中的 IP 主机的流量。另外 SMON Ⅱ还可以对每一种应用协议进行流量监控。第一个采用 SMON Ⅱ标准的多层交换机是朗讯(后来更名为 AVAYA)公司的 Cajun M770 M-MLS。目前主流的三层交换机都采用 SMON Ⅱ标准。

RMON 与 SMON 的监控内容相似,主要对数据链路层的流量进行统计;而 RMON Ⅱ与 SMON Ⅱ的监控内容相似,支持网络层及以上各层(主要在应用层)的性能监控。例如,在企业网络的出口处,通过对与 Internet 连接的端口的网络层流量的监控,可以了解局域网出口的流量大小。同时,还可以针对应用层的 HTTP、SMTP、FTP 等流量进行监

控，了解每一种协议应用所使用的流量情况。

一个标准的RMONⅡ探测器对一个网段的全部流量进行监控而不加区分，而SMONⅡ可以根据交换机的路由状态表记录数据信息，这种信息可以被看作一个单一的数据源。这样，SMON Ⅱ就可以实现对具体协议、VLAN的分类统计。更具体来讲，在SMON Ⅱ的网络管理环境中，网络管理员可以完成以下几项工作：

(1) 根据管理需要，管理员可以定义所要监控的OSI模型的层次，同时也可以定义应用层的协议类型。

(2) 对整个交换机内不同协议的流量占用情况进行实时统计和分析。

(3) 对与交换机相连的IP和IPX子网上的流量进行监控，所以SMON Ⅱ不但能够监控IP流量的详细情况，而且可以监控IPX等非IP流量的大小。

(4) 对主机之间(同一网段或不同网段)的通信流量进行监控。

1.3 Windows操作系统的用户和桌面管理技术

网络已从对互联设备的松散集成，发展为由相互依存的资源所组成的复杂生态系统。为此，网络操作系统所要提供的服务将远远不止是简单的网络文件与打印服务，而应更进一步地提供对分布式网络资源进行透明化管理的工具。

1.3.1 活动目录

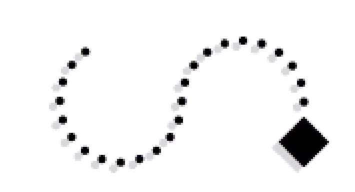
活动目录(Active Directory，AD)，是从Windows 2000开始引入的操作系统的重要组件。AD可以认为是一个大的层次结构数据库，用来集中存储企业内部的用户账户、计算机、打印机、应用程序、安全性与系统原则等各种重要资源。AD允许网络用户通过单一登录就可以访问网络中任何位置的许可资源。

活动目录是Windows内置的目录服务，是其网络体系的基本结构模型及核心支柱。不管用户从何处访问或信息处在何处，都对用户提供统一的视图。它也是一个企业级的目录服务，具有很好的可伸缩性。活动目录以轻目录访问协议(LDAP)作为基础，支持X.500中定义的目录体系结构，并具有可复制、可分区及分布式的特点。

1. 逻辑结构

逻辑结构是指非物理上的、非实体的东西，它是一种抽象的东西，例如讲一种“关系”、一个“空间、范围”等。活动目录的逻辑结构非常灵活，有目录树、域、域树、域林等，这些名字都不是实实在在的一种实体，只是代表了一种关系，一种范围，如目录树就是由同一名字空间上的目录组成的，而域又是由不同的目录树组成的，同理域树是由不同的域组成的，域林是由多个域树组成的。它们是一种完全的树状、层次结构视图，这种关系我们可以看成一种动态关系。逻辑结构还与前面讨论过的名字空间有直接的关系，逻辑结构为用户和管理员在一定的名字空间中查找、定位对象提供了极大的方便。

(1) 域既是Windows网络系统的逻辑组织单元，是对象(如计算机、用户等)的容器，这些对象有相同的安全需求、复制过程和管理。在Windows域中所有的域控制器都是平等的，域是安全边界，域管理员只能管理域的内部，除非其他的域显式地赋予他管理权限，



他才能够访问或管理其他的域。

每个域都有自己的安全策略,以及它与其他域的安全信任关系。域与域之间具有一定的信任关系,域信任关系使得一个域中的用户可由另一域中的域控制器进行验证,才能使一个域中的用户访问另一个域中的资源。所有域信任关系中只有两种域:信任关系域和被信任关系域。信任关系就是域 A 信任域 B,则域 B 中的用户可以通过域 A 中的域控制器进行身份验证后访问域 A 中的资源,则域 A 与域 B 之间的关系就是信任关系。

被信任关系就是被一个域信任的关系,在上面的例子中域 B 被域 A 信任,域 B 与域 A 的关系就是被信任关系。信任与被信任关系可以是单向的,也可以是双向的,即域 A 与域 B 之间可以是单方面的信任关系,也可以是双方面的信任关系。

当多个域通过信任关系连接起来之后,所有的域共享公共的表结构(schema)、配置和全局目录(Global Catalog),从而形成域树 。域树由多个域组成,这些域共享同一个表结构和配置,形成一个连续的名字空间。树中的域通过信任关系连接起来。活动目录包含一个或多个域树。

域森林是指一个或多个没有形成连续名字空间的域树。域林中的所有域树共享同一个表结构、配置和全局目录。域林中的所有域树通过 Kerberos 信任关系建立起来,所以每个域树都知道 Kerberos 信任关系,不同域树可以交叉引用其他域树中的对象。

(2) 组织单元(OU)是一个容器对象,它也是活动目录的逻辑结构的一部分,我们可以把域中的对象组织成逻辑组,它可以帮助我们简化管理工作。OU 可以包含各种对象,如用户账户、用户组、计算机、打印机等,甚至可以包括其他的 OU,所以我们可以利用 OU 把域中的对象形成一个完全逻辑上的层次结构。对于企业来讲,可以按部门把所有的用户和设备组成一个 OU 层次结构,也可以按地理位置形成层次结构,还可以按功能和权限分成多个 OU 层次结构。

很明显,通过组织单元的包容,组织单元具有很清楚的层次结构,这种包容结构可以使管理者把组织单元切入域中以反映出企业的组织结构并且可以委派任务与授权。建立包容结构的组织模型能够帮助我们解决许多问题,同时仍然可以使用大型的域、域树中的每个对象都可以显示在全局目录,从而用户就可以利用一个服务功能轻易地找到某个对象而不管它在域树结构中的位置。

由于 OU 层次结构局限于域的内部,所以一个域中的 OU 层次结构与另一个域中的 OU 层次结构没有任何关系。一个企业有可能只用一个域来构造企业网络,这时候我们就可以使用 OU 来对对象进行分组,形成多种管理层次结构,从而极大地简化网络管理工作,如图 1-3 所示。组织中的不同部门可以成为不同的域,或者一个组织单元,从而采用层次化的命名方法来反映组织结构并进行管理授权。顺着组织结构进行颗粒化的管理授权可以解决很多管理上的头疼问题,在加强中央管理的同时,又不失机动灵活性。

2. 物理结构

微软活动目录中,物理结构与逻辑结构有很大的不同,它们是彼此独立的两个概念。逻辑结构侧重于网络资源的管理,而物理结构则侧重于网络的配置和优化。活动目录的物理结构主要着眼于活动目录信息的复制和用户登录网络时的性能优化。物理结构的两个重要概念是站点和域控制器。

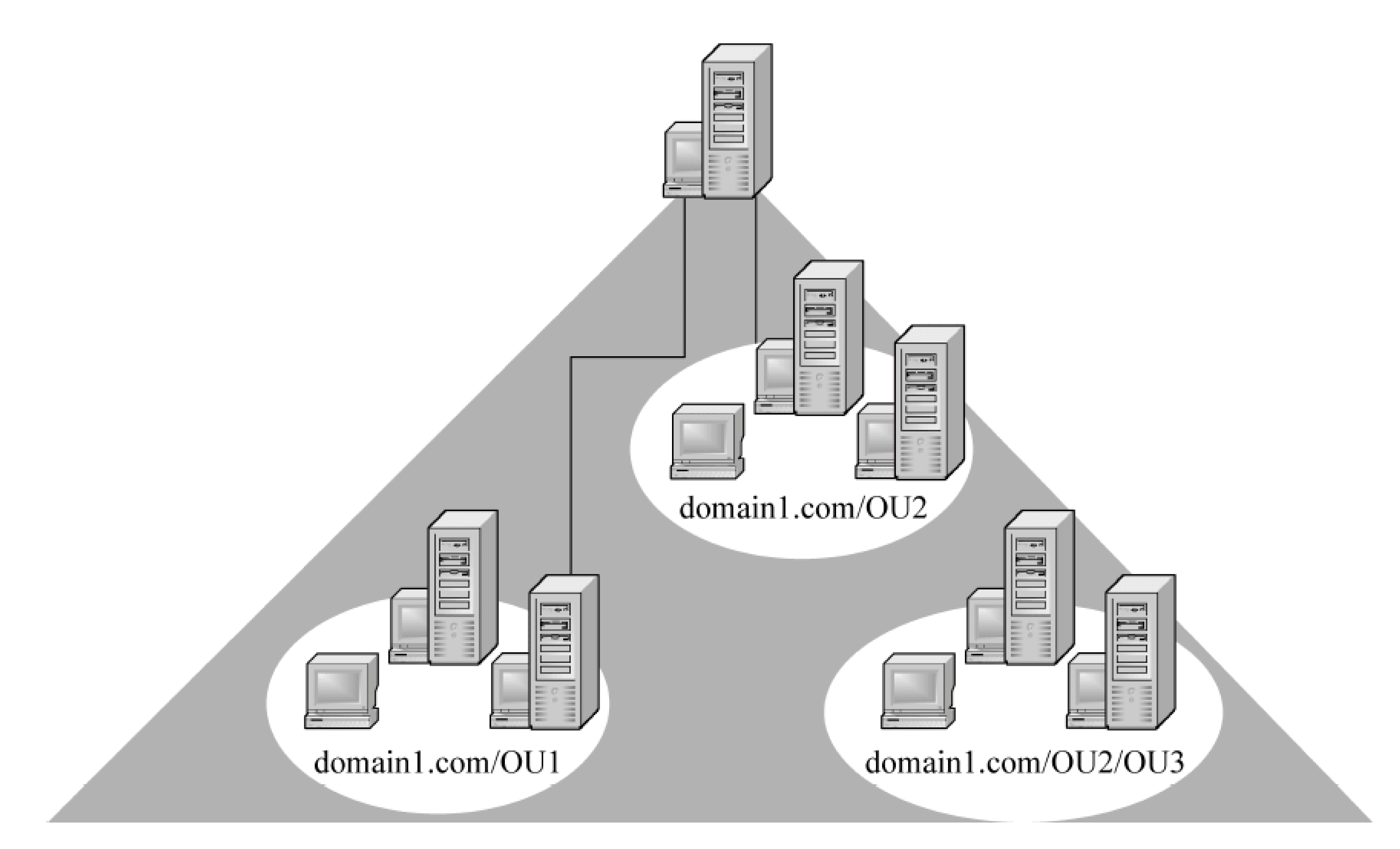


图 1-3　组织结构的层次结构

（1）站点是由一个或多个 IP 子网组成的，这些子网通过高速网络设备连接在一起。站点往往由企业的物理位置分布情况决定，可以依据站点结构配置活动目录的访问和复制拓扑关系，这样能使得网络更有效地连接，并且可使复制策略更合理，用户登录更快速，活动目录中的站点与域是两个完全独立的概念，一个站点中可以有多个域，多个站点也可以位于同一域中。

活动目录站点和服务可以通过使用站点提高大多数配置目录服务的效率。可以通过使用活动目录站点和服务向活动目录发布站点的方法提供有关网络物理结构的信息，活动目录使用该信息确定如何复制目录信息和处理服务的请求。计算机站点是根据其在子网或一组已连接好的子网中的位置指定的，子网提供一种表示网络分组的简单方法，这与我们常见的邮政编码将地址分组类似。将子网格式化成可方便发送有关网络与目录连接物理信息的形式，将计算机置于一个或多个连接好的子网中充分体现了站点所有计算机必须连接良好这一标准，原因是同一子网中的计算机的连接情况通常优于网络中任意选取的计算机。

（2）域控制器是指运行 Windows Server 版本的服务器，它保存了活动目录信息。域控制器管理目录信息的变化，并把这些变化复制到同一个域中的其他域控制器上，使各域控制器上的目录信息处于同步。域控制器也负责用户的登录过程以及其他与域有关的操作，如身份鉴定、目录信息查找等一个域可以有多个域控制器。规模较小的域可以只需要两个域控制器，一个实际使用；另一个用于容错性检查。规模较大的域可以使用多个域控制器。

1.3.2　组策略

组策略（Group Policy）是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。组策略

是 Windows 中的一套系统更改和配置管理工具的集合。注册表是 Windows 系统中保存系统软件和应用软件配置的数据库，而组策略则将系统重要的配置功能汇集成各种配置模块，供用户直接使用，从而达到方便管理计算机的目的。

组策略的设置数据保存在 AD 数据库中，因此必须在域控制器上设置组策略。组策略只能够管理计算机与用户。也就是说组策略是无法管理打印机、共享文件夹等其他对象的。组策略不能应用到组，只能够应用到站点、域或组织单位（SDOU）。组策略不会影响未加入域的计算机和用户，对于这些计算机和用户，应使用本地安全策略来管理。

1. 组策略的设置数据

组策略的设置数据都是保存在“组策略对象”（GPO）中，GPO 具有以下特性：

（1）GPO 利用 ACL 记录权限设置，可以修改个别 GPO 的 ACL，指定哪些人对该 GPO 拥有何种权限。

（2）用户只要有足够的权限，便能够添加或删除 GPO，但无法复制 GPO。当 AD 域刚建好时，默认仅有一个 GPO——DEFAULT DOMAIN POLICY。这个 GPO 可用来管理域中所有的计算机与用户。若要设置应用于组织单位的组策略，通常会再另行建立 GPO，以方便管理。

（3）GPO 本身保存组策略的设置值，必须要进一步指定 GPO 连接哪一个 SDOU，才能使组策略在应用对象生效。GPO 与 SDOU 间的连接关系如图 1-4 所示，可以是一对一，一对多或多对一。



图SDOU 间的连接关系

2. GPO 的两大类策略

（1）计算机设置：包含所有与计算机有关的策略设置，这些策略只会应用到计算机账户。

（2）用户设置：包含所有与用户有关的策略设置，这些策略只会应用到用户账户，如图 1-5 所示。

3. 组策略的应用机制

两项特性：继承与累加。

策略继承：在 AD 结构中，若 X 容器下层还有 Y 容器，则 Y 容器便是所谓的“子容器”，X，Y 容器两者间便存在策略关系。在默认情况下子容器会继承来自上层容器的 GPO。在整个继承关系中，最上层为站点，其下层为域与组织单位。若有多层组织单位，则下层组织单位会继承上层组织单位的 GPO，如图 1-6 所示。

策略累加：策略累加机制和组策略的应用顺序有密切的关系。子容器会首先应用继承来自上层容器的组策略，然后再应用本身的组策略，当上层的设置项目与下层的设置项目不同时，组策略的效果可以相加，但若是对同一个项目做不同的设置，则先应用的策略会被后来应用的策略覆盖。但是我们可以根据实际应用需求去人为地干预默认的继承规则，可以阻止或强制继承。

阻止继承：在“组策略管理”控制台中，右键选择是否继承上一级容器组策略的容器，

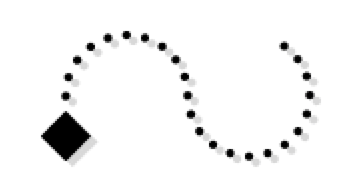




图 1-5　组策略的内容

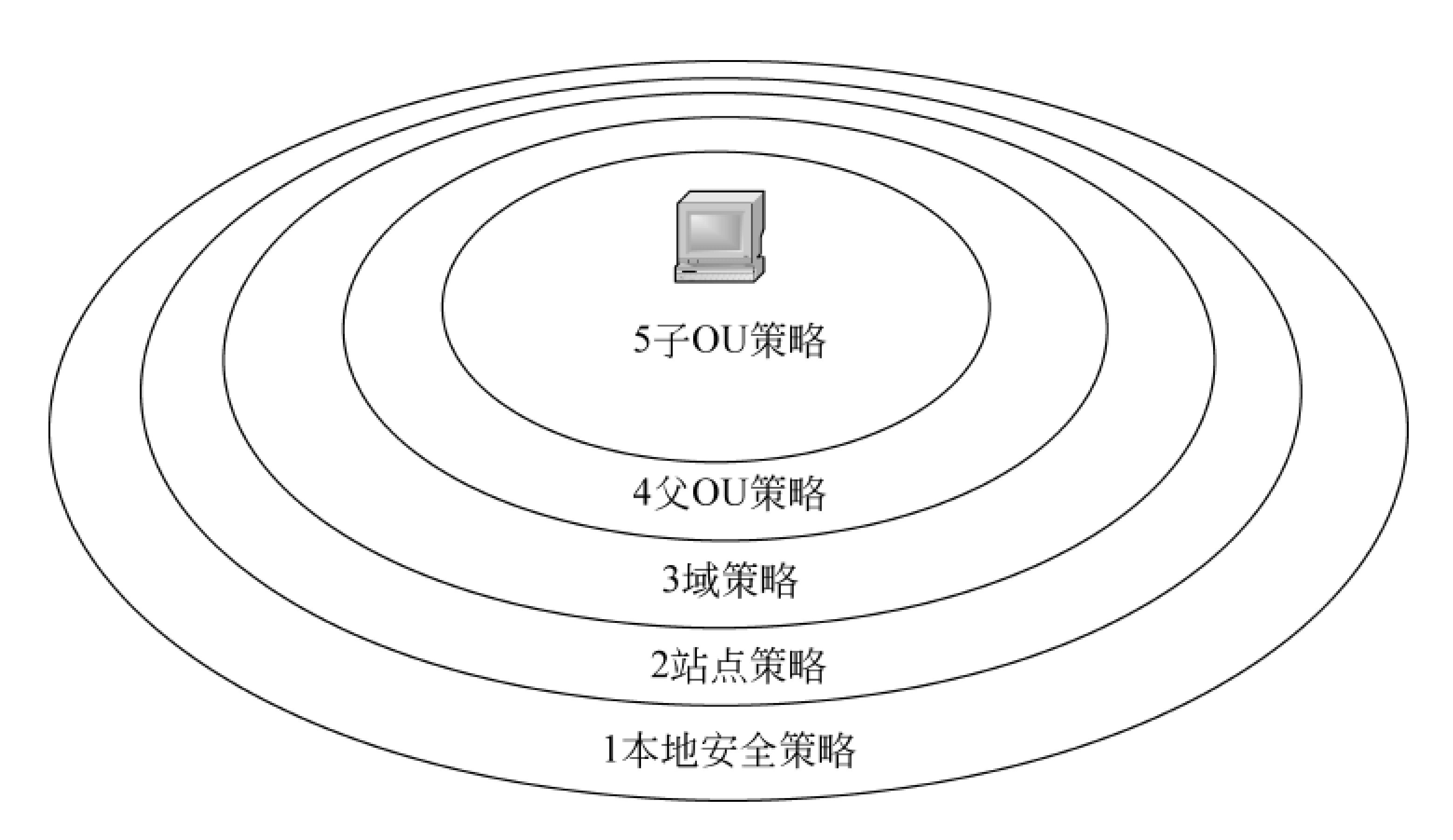
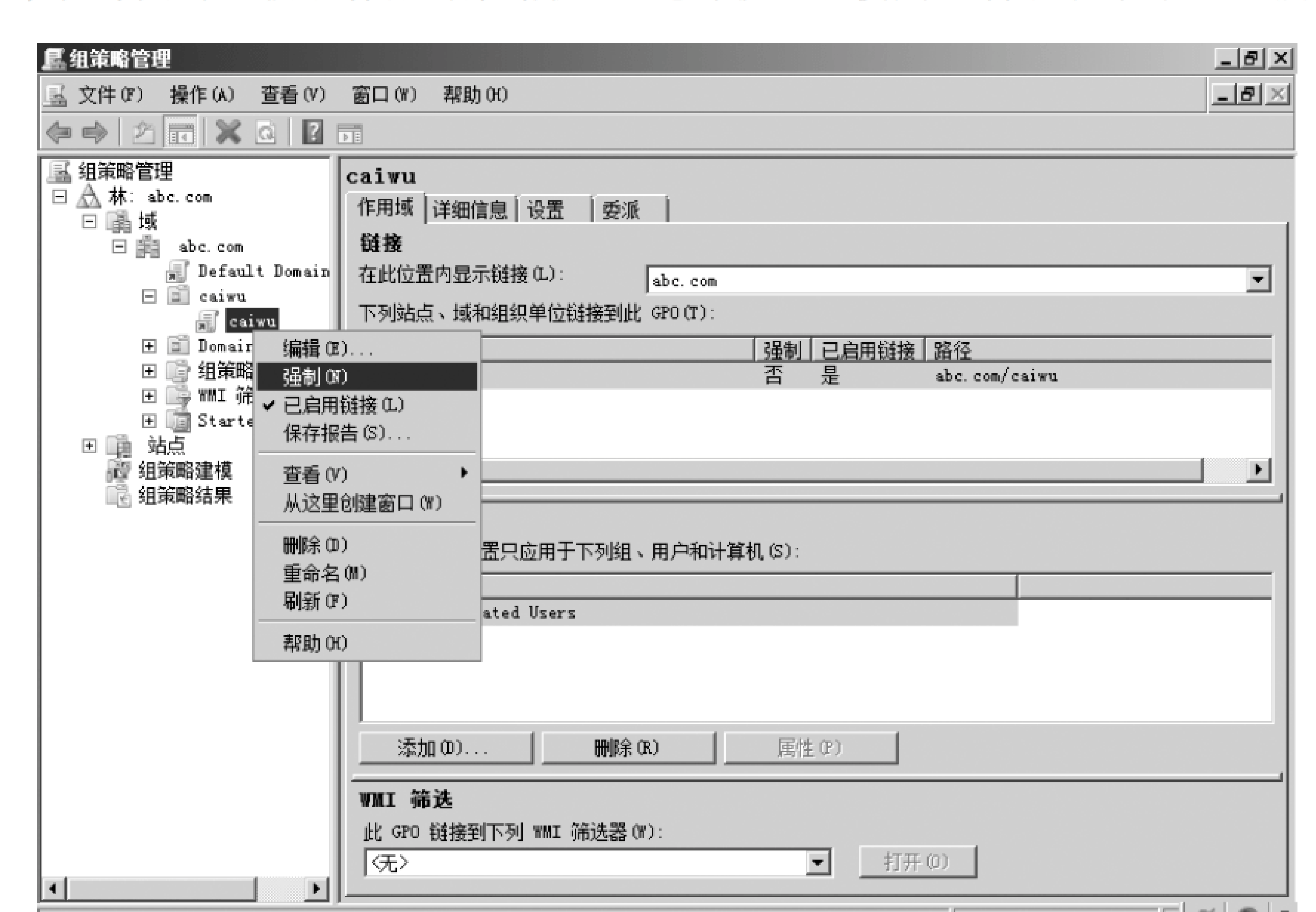
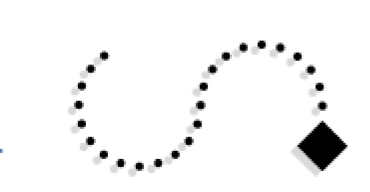


图 1-6　组策略的继承关系

选择“阻止继承”,如图 1-7 所示。

强制继承:在实际应用中有时需要上一级容器的组策略配置被应用到子容器中去,并且要求在冲突时不被子容器的策略覆盖,这时就可以使用强制继承,如图 1-8 所示。





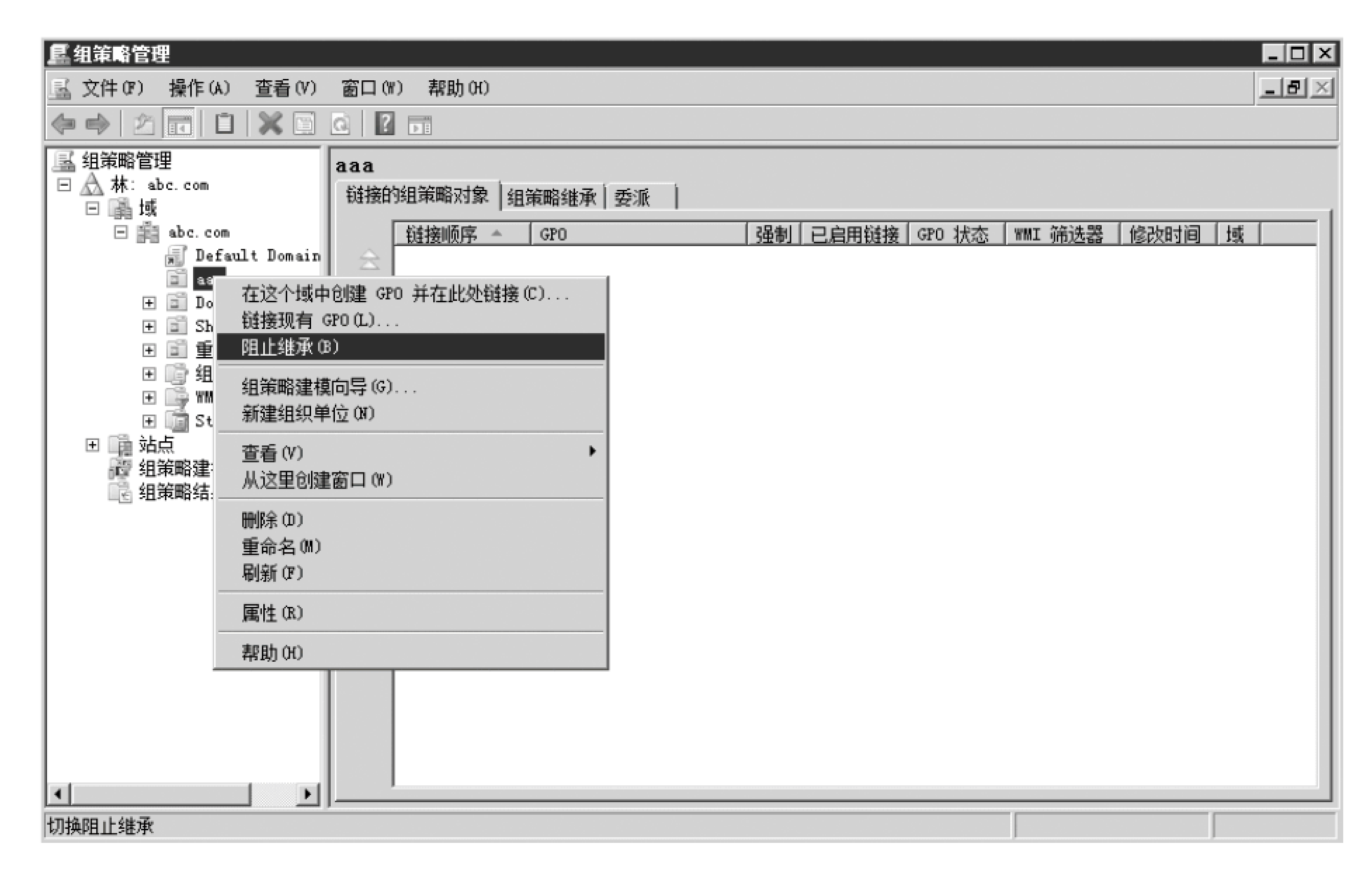


图 1-7　阻止继承

1.4　基于局域网的网络监控软件

随着计算机网络技术的普及,网络在信息的采集、加工和处理上起着越来越重要的作用。但如何规范网络使用者的行为,保证网络上的信息安全是一个亟待解决的问题,网络监控软件在这方面进行了有益的探索。

1.4.1　网络监控软件概述

网络监控软件是指针对局域网内的计算机进行监视和控制;针对内部计算机上的互联网以及内部行为与资产等过程管理。局域网监控的有效范围是以监控点为基点半径没有跨越路由范围的局域网。因为局域网监控需要捕获 ISO 模型中的第二层数据包(MAC 层帧)以解析网络传输包协议以及确认监视对象需求,而穿过路由后就无法捕获了。因此我们能简单地理解 Internet 用户之间是不能互相监视的,能做的只是监控自己本单位范围的计算机。

局域网外网监控软件(上网行为管理、网络行为审计、内容监视、上网行为控制)应包含以下基本功能：通过局域网内任何一台计算机监视、记录、控制其他计算机的上网行为;能实现上网监控、网页浏览监控、邮件监控、Webmail 发送监视、聊天监控、BT 禁止、流量监视、上下行分离流量带宽限制、并发连接数限制、FTP 命令监视、FTP 内容监视、FTP 行为控制、Telnet 命令监视、网络行为审计、操作员审计、软网关功能、端口映射和 PPPOE 拨号支持、通过 Web 方式发送文件的监视、通过 IM 聊天工具发送文件的监视和控制等。

用于全程监视和控制管理网络内所有用户上外网的过程。能够探测、拦截、收集、禁

止和管理整个上网资源，规范网络有效合法使用。防止单位重要资料、机密文件等的泄密；监督审查网络使用行为；备份重要网络资源文件；限制邮件、网站、聊天、游戏、股票、下载、流量以及自定义网络应用等行为，并可以作为软网关运行。

局域网内网监控软件（内网行为管理、屏幕监视、软硬件资产管理、数据安全）应包含以下基本功能：用于监视计算机开机后的所有操作情况，能够全程管理和控制内网计算机的全部过程；支持内网监控、屏幕监视和录像、软硬件资产管理、光驱和 USB 等硬件禁止、应用软件限制、打印监控、ARP 防火墙、消息发布、日志报警、远程文件自动备份功能、禁止修改本地连接属性、禁止聊天工具传输文件、禁止修改本地连接属性、通过网页发送文件监视、远程文件资源管理、支持远程关机注销等；一般情况下，内网监控需要在被监视计算机安装工作站软件。

1.4.2 外网监控中使用的主要技术

1. 数据侦听技术

(1) 网关模式：原理是把本机作为其他电脑的网关（设置被监视计算机的默认网关指向本机），分别可以作为单网卡方式和双网卡甚至多网卡方式，原始的 Proxy 模式淘汰后已不再有人采用，常用的是 NAT 存储转发的方式；简单说有点像路由器工作的方式；控制力强，由于存储转发的方式，性能有些损失；效率好；缺陷是网关坏了，全网就瘫痪了。

(2) 网桥模式：原理是双网卡做成透明桥，而桥是工作在第二层的，所以可以简单理解为桥为一条网线，因此性能是最好的，几乎没有损失；WinPcap 本身并不支持该模式；该模式可以说是最理想的了，即使桥坏了，只要简单做个跳线就可以了，因为桥是透明的，可以看成网线，桥坏了可以理解为网线坏了，只需换一条而已；支持多 VLAN、无线、VPN、多出口等几乎所有的网络情况。

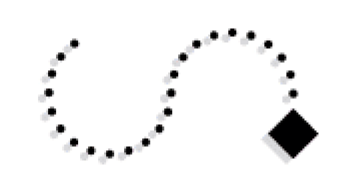
(3) 旁路模式：原理是使用 ARP 技术建立虚拟网关，只能适合于小型的网络，并且环境中不能有限制旁路模式；路由或火墙的限制或被监视计算机安装了 ARP 火墙都会导致无法旁路成功；但该方式是最简单的部署以及最方便的安装设置。

(4) 旁听模式：原理是旁路监听，是通过交换机的镜像功能来实现监控的，该模式需要采用共享式 Hub 或交换机镜像；可是如果采用老式的共享式 Hub 将影响网络出口性能；如采用镜像模式，一方面需要投资支持双向的镜像交换机设备；另一方面需要专业的人设置镜像交换机。该模式的优点是部署方便灵活，只要在交换机上配置镜像端口即可，不需要改变现有的网络结构；而且旁路监控设备一旦停止工作，也不会影响网络的正常运行。缺点在于，旁听模式通过发送 RST 包只能断开 TCP 连接，不能控制 UDP 通信，如果要禁止 UDP 方式通信的软件，需要在路由器上做相关设置进行配合。

2. Windows 平台上获取数据包技术

Windows 平台上获取数据包技术主要包括核心层驱动和网络层驱动两种方式。

(1) 核心层驱动和 Windows 操作系统核心结合紧密，效率非常高、性能最好；因为网络防火墙都在网络上层运行（也就是说在防火墙核心层驱动上面运行），因此核心层驱动将不受网络防火墙干扰；功能更加强大，性能更好；如 Kercap 驱动标准接口、Anyview Nat Service 内核驱动。



Kercap 内核抓包驱动引擎是国内自主研发的具有世界领先水平的 Windows 内核驱动程序，利用 IMD 技术实现的 Kercap 内核抓包引擎在稳定 他 技术实现方式有极大的优势，比传统的 WinPcap 内核程序 大 的网络抓包。

Anyview Nat Service 是国内自主研发并且是世界最先 核 驱动引擎之一，十年以上实际批量规模运行。该技术采用 IS 内核驱动技术，类似卡巴斯基的内核技术直接嵌入 Windo 防 火墙干扰，并比网络层驱动快百倍以上。更强大的性能，更 的 功能，更好的性能；可以支持成千上万个计算机的同时监控

（2）网络层驱动，虽然容易控制管理但性能根本无法 火 墙限制和干扰；实例如 WinPcap 驱动接口。

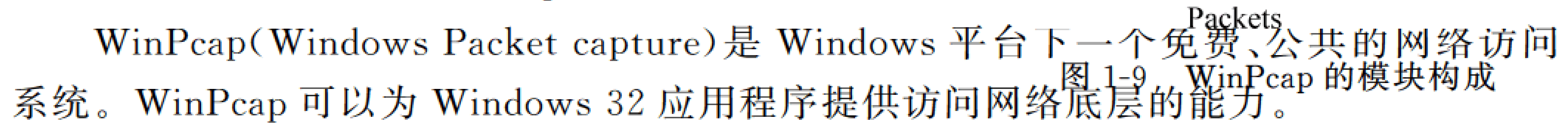


图 1-9　WinPcap 的模块构成

WinPcap（Windows Packet capture）是 Windows 平台下一个免费、公共的网络访问系统。WinPcap 可以为 Windows 32 应用程序提供访问网络底层的能力。

它提供了以下的各项功能：

- 捕获原始数据包，包括网络上各主机发送/接收的以及相互之间交换的数据包；
- 在数据包发往应用程序之前，按照自定义的规则将某些特殊的数据包过滤掉；
- 在网络上发送原始的数据包；
- 收集网络通信过程中的统计信息。

WinPcap 由三个模块构成，如图 1-9 所示。

- NPF（Netgroup Packet Filter）即网络组包过滤器：它是运行于操作系统内核中的驱动程序，直接与网卡驱动程序进行交互，获取网络上传输的原始数据包。同时还可以发送、存储数据包以及对网络进行统计分析。
- Packet. dll 动态链接库：它为 Windows 32 平台提供了一个公共的接口，不同版本的 Windows 系统都有自己的内核模块和用户层模块。Packet. dll 用于解决这些不同，调用 Packet. dll 的程序可以运行在不同版本的 Windows 平台上而无须重新编译。
- Wpcap. dll 高级动态链接库：该动态链接库比 Packet.dll 更高级，它的调用与操作系统无关，它和应用程序编译在一起，使用由 Packet.dll 提供的服务，向应用程序提供完善的接口函数，提供了更高层、更抽象的函数。

WinPcap 是目前免费的接口程序，支持 100M 通信。但缺点也同样是明显的，可控制性很差导致很多功能都无法实现。只能在监听模式工作，无法实现网关模式下运行，导致流量限制、BT 限制、UDP 阻断方面等天生的弱点。另外由于 WinPcap 版本互相不兼容可能导致无法监控、无法识别千兆网卡或无法读到网卡列表等。

3. 业务识别技术

（1）普通报文分析。

普通“报文检测”仅分析数据包的第二至第四层的内容，包括源地址、目的地址、源端口、目的端口以及协议类型。普通报文检测是通过端口号来识别应用类型的，如检测到端口号为 80 时，就认为该应用代表着普通上网应用。

（2）基于“特征字”的识别技术。

不同的应用通常依赖于不同的协议，而不同的协议都有其特殊的指纹，这些指纹可能是特定的端口、特定的字符串或者特定的比例序列。基于“特征字”的识别技术通过对业务流中特定数据报文中的“指纹”信息的检测以确定业务流承载的应用。

根据具体检测方式的不同，基于“特征字”的识别技术又可以分为固定位置特征字匹配、变动位置特征匹配以及状态特征匹配三种技术。

通过对“指纹”信息的升级，基于特征的识别技术可以很方便地进行功能扩展，实现对新协议的检测。

如 Bittorrent 协议的识别，通过反向工程的方法对其对等协议进行分析，所谓对等协议指的是 peer 与 peer 之间交换信息的协议。对等协议由一个握手开始，后面是循环的消息流，每个消息的前面，都有一个数字来表示消息的长度。在其握手过程中，首先是发送 19，跟着是字符串 BitTorrent Protocol。那么 19 Bit Torrent Protocol 就是 Bittorrent 的“特征字”。

（3）应用层网关识别技术。

某些业务的控制流和业务流是分离的，业务流没有任何特征。这种情况下，我们就需要采用应用层网关识别技术。

应用层网关需要先识别出控制流，并根据控制流的协议通过特定的应用层网关对其进行解析，从协议内容中识别出相应的业务流。

对于每一个协议，需要有不同的应用层网关对其进行分析。

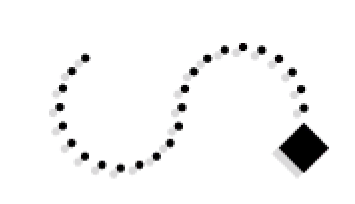
如 SIP、H323 协议都属于这种类型。SIP/H323 通过信令交互过程，协商得到其数据通道，一般是 RTP 格式封装的语音流。也就是说，纯粹检测 RTP 流并不能得出这条 RTP 流是通过哪种协议建立的。只有通过检测 SIP/H323 的协议交互，才能得到其完整的分析。

（4）行为模式识别技术。

行为模式识别技术基于对终端已经实施的行为的分析，判断出用户正在进行的动作或者即将实施的动作。行为模式识别技术通常用于无法根据协议判断的业务的识别。例如：SPAM（垃圾邮件）业务流和普通的 E-mail 业务流从 E-mail 的内容上看是完全一致的，只有通过对用户行为的分析，才能够准确地识别出 SPAM 业务。

本章小结

本章主要讲述了计算机网络管理概念、功能和实现网络管理所使用的主要技术。要求学生理解 SNMP 的体系结构和主要思想，了解 Windows 操作系统用活动目录和组策略对网络用户和桌面进行管理的技术，了解局域网监控软件的作用和其中涉及的主要技术，从而对网络管理技术有一个总体的理解，为后续的学习打下一个良好的基础。



本章习题

1. 简述网络管理的主要功能和网管软件的分类。
2. 简述 SNMP 的基本内容。
3. 简述活动目录的逻辑结构和物理结构。
4. 简述组策略内容和应用机制。
5. 简述局域网监控软件包含的主要技术。

第 2 章

活动目录管理

【本章重点】

掌握活动目录进行局域网管理的基本思想,活动目录域服务的层级结构。掌握活动目录中各实体的管理理论和基本概念。通过实例掌握在活动目录中域、子域、用户、组、OU 的设置和管理方法。

2.1 活动目录中的基础概念

活动目录是指集中的、安全的存储网络资源信息的目录,以及让这些信息可供网络用户使用的所有服务。网络中的所有资源包括用户账户、文件数据、打印机、服务器、数据库、组、计算机和安全策略等,这些都可以存储在活动目录中。

我们也可以把活动目录理解为一个存储仓库,以计算机为操作工具,账户和资源用统一的命名、描述、定位集中管理起来并保证这些数据的安全。活动目录通过域、组织单位、组、账户等组成它的逻辑空间,图 2-1 是活动目录的一个示例。

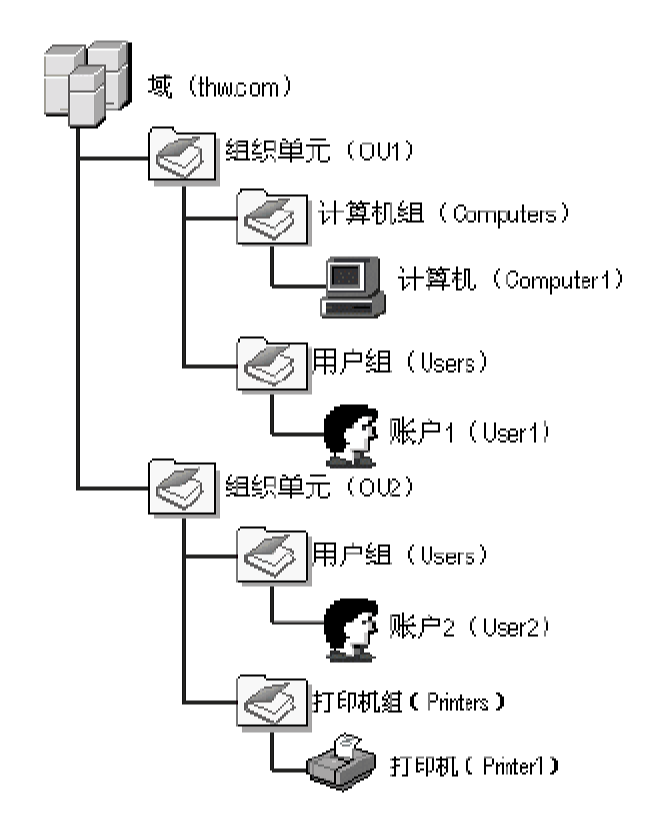


图 2-1 活动目录示例

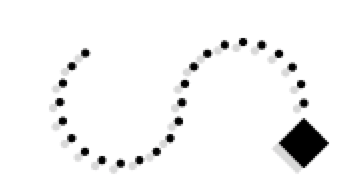
2.1.1 域模式下用户与用户组管理

1. 域模式管理原理

微软公司在其网络操作系统中采用了域模式来提高管理效率,其核心就在于将计算机加入一个指定的逻辑单元——域中,然后对加入其的计算机实现统一、高效的管理,域对整个网络系统中的计算机、用户、资源重新进行了整合,以方便管理员和计算机用户的管理与使用。

在域模式的管理体系下,整个网络管理经过以下 4 个过程实现对加入域的所有计算机和用户的综合管理。

(1) 建立一个域和域管理员,如图 2-2 所示。



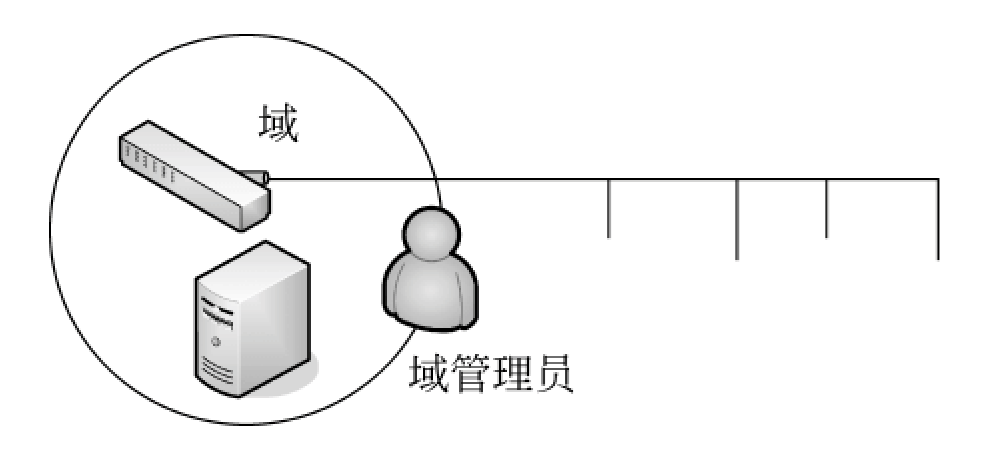


图 2-2 建立域和域管理员

(2) 将被管理的计算机加入域中，如图 2-3 所示。

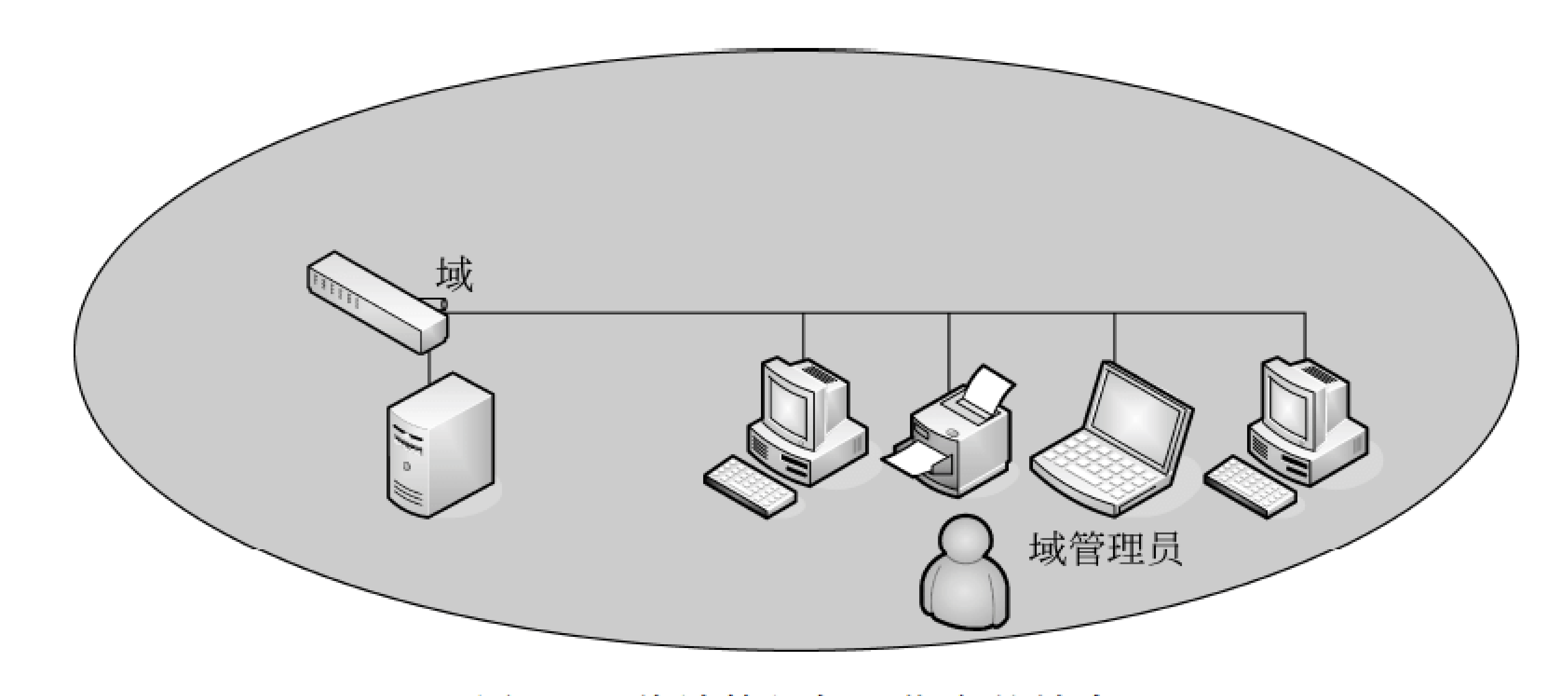


图 2-3 将计算机加入指定的域中

(3) 使用域下的管理员账户建立新的用户，如图 2-4 所示。

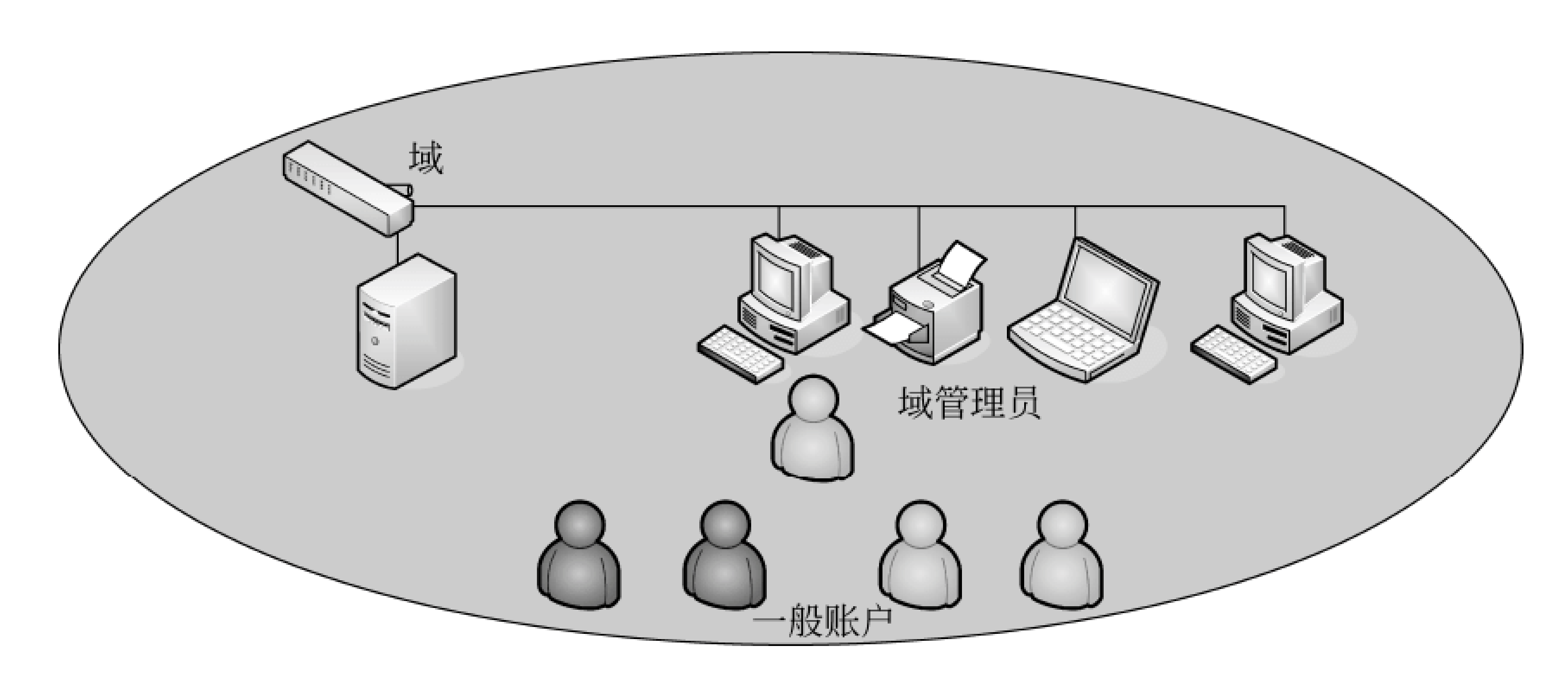


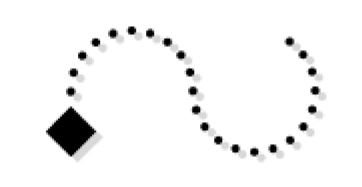
图 2-4 域管理员在域中创建账户

(4) 在域中通过任何计算机对域中的任何账户实现设置管理，如图 2-5 所示。

从以上步骤和图示中可以看出，当计算机加入域成为域模式下的一台客户机时，针对该计算机的管理和针对用户的管理一下子就变得简单了，最终所有用户都可以通过任意指定的计算机访问任意计算机上的文件夹且运行权限允许的可执行文件。

2. 域模式下的用户设置

当一台计算机成为域控制器时，或者当一台计算机加入的域成为域模式下的一台客户机时，每台计算机中的账户信息将发生改变。



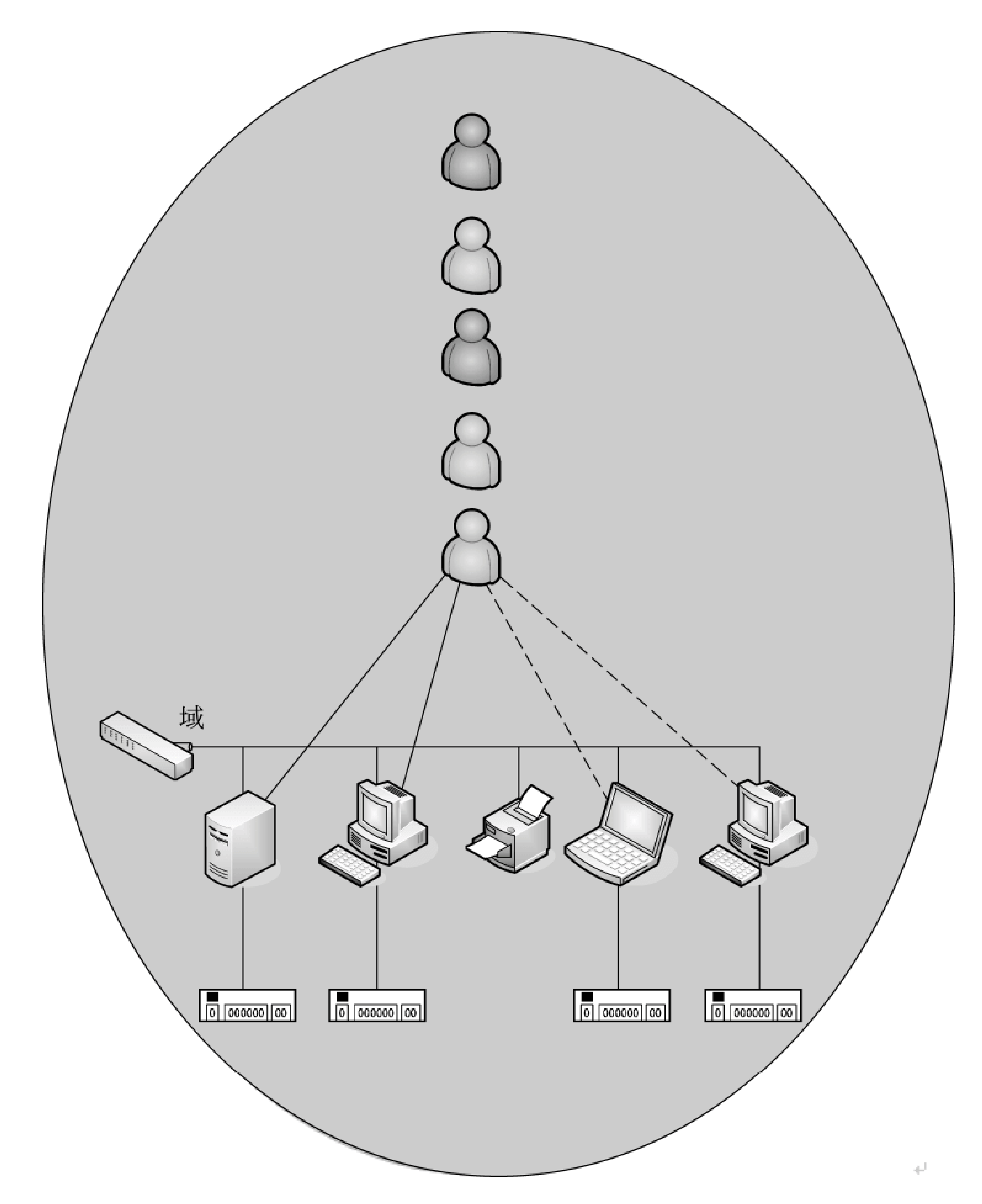


图 2-5　在域中通过域中任何计算机实现设置管理

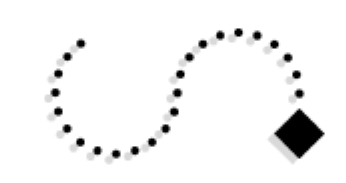
(1) 在域控制器中，原本地账户已经不能使用了。因为，原本地管理员的账户继续存在将有可能破坏域服务器，因此对域控制器的管理和控制交由域控制器管理员完成。域控制器管理界面，如图 2-6 所示。

当域管理员登录域控制器时，在域控制器中出现了新的账户管理界面。选择"开始"→"程序"→"管理工具"后出现了新的功能选项"Active Directory 用户和计算机"，如图 2-7 所示，选择该命令可进入域控制器账户的管理界面。

在网络中将计算机升级到 Active Directory 服务器后，系统中"管理工具"的"计算机管理"选项将无法使用，而增加了一项"Active Directory 用户和计算机"选项，而原来的"本地用户"将迁移到 Active Directory 用户中，域用户将有更多的属性。

在域模式管理计算机的网络中，需要为使用计算机的每个人创建一个域用户账户。当一台计算机成为域控制器，一台计算机加入的域成为域模式下的一台客户机时，每台计算机中的账户信息将发生改变。

当域管理员登录域控制器时在域控制器中出现了新的账户管理界面。在进入"管理



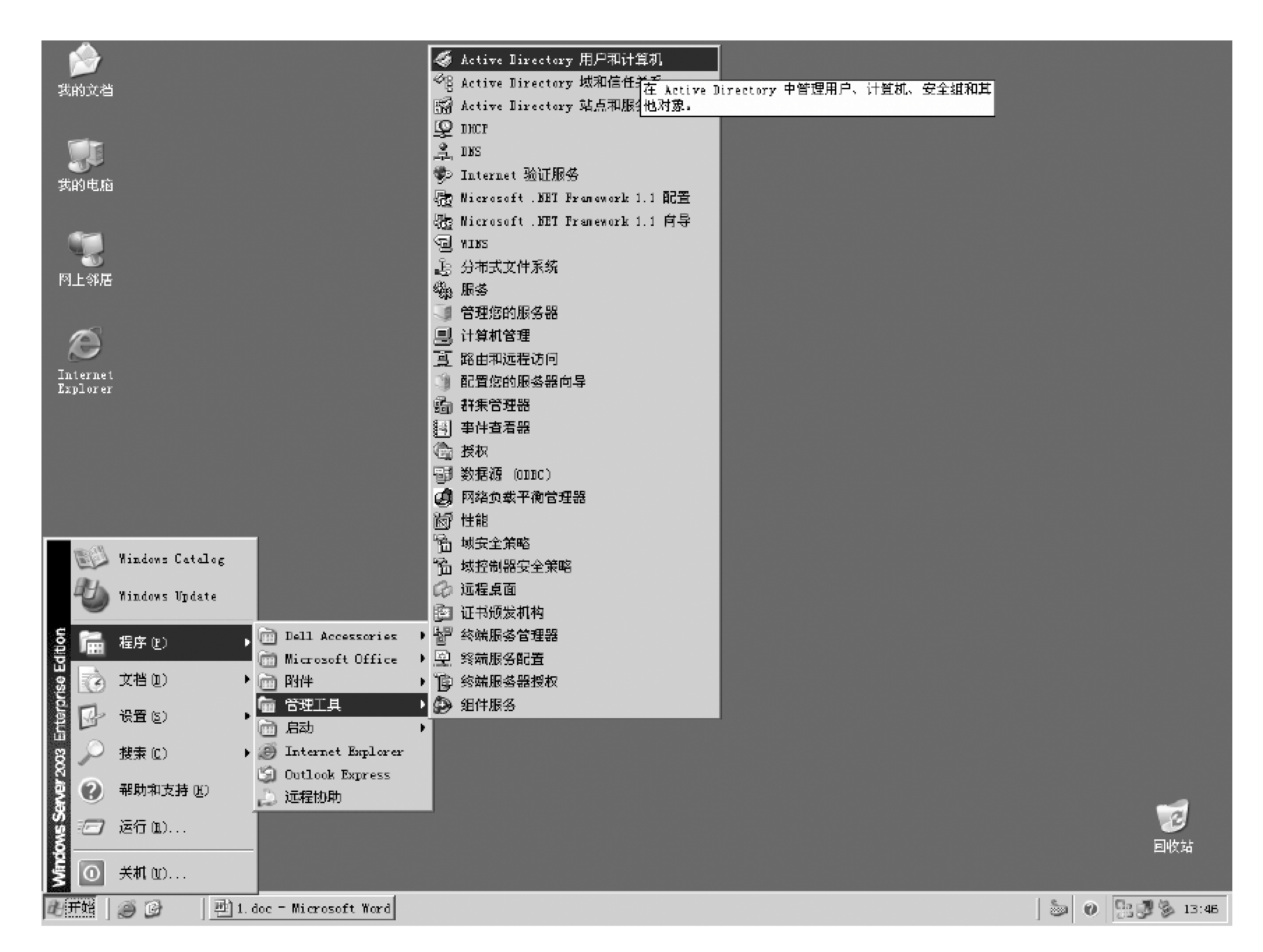


图 2-6　域控制器管理界面

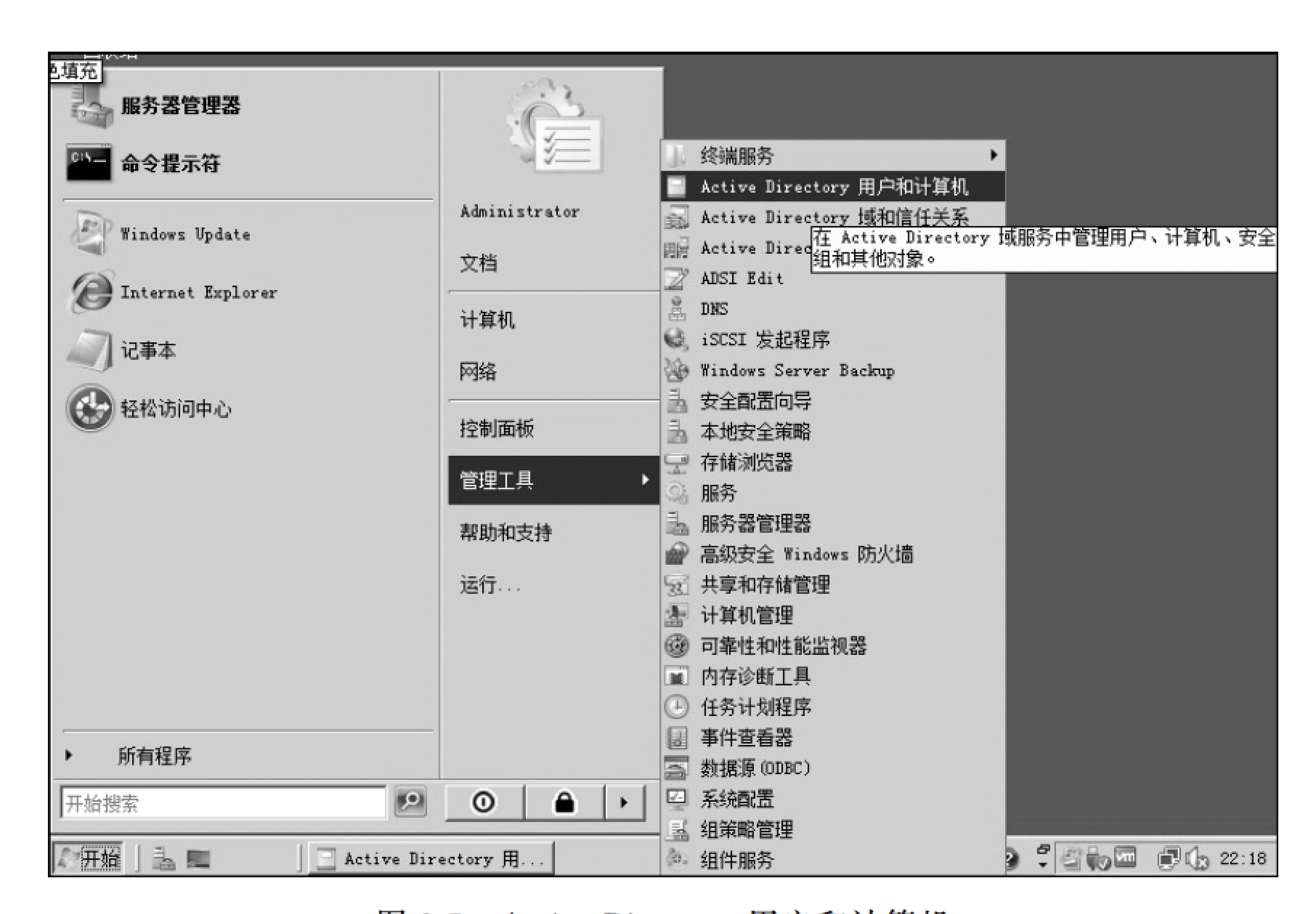


图 2-7　Active Directory 用户和计算机

工具"后出现了新的功能图标"Active Directory 用户和计算机",如图 2-8 所示,单击该图标即可进入域控制器账户的管理界面。

(2) 通过客户机进入域控制器前,系统出现两个进入选项,一个是本地机进入选项,一个是域控制器选项,如图 2-9 所示,作为客户机如果不进入域环境则选择本地机选项,

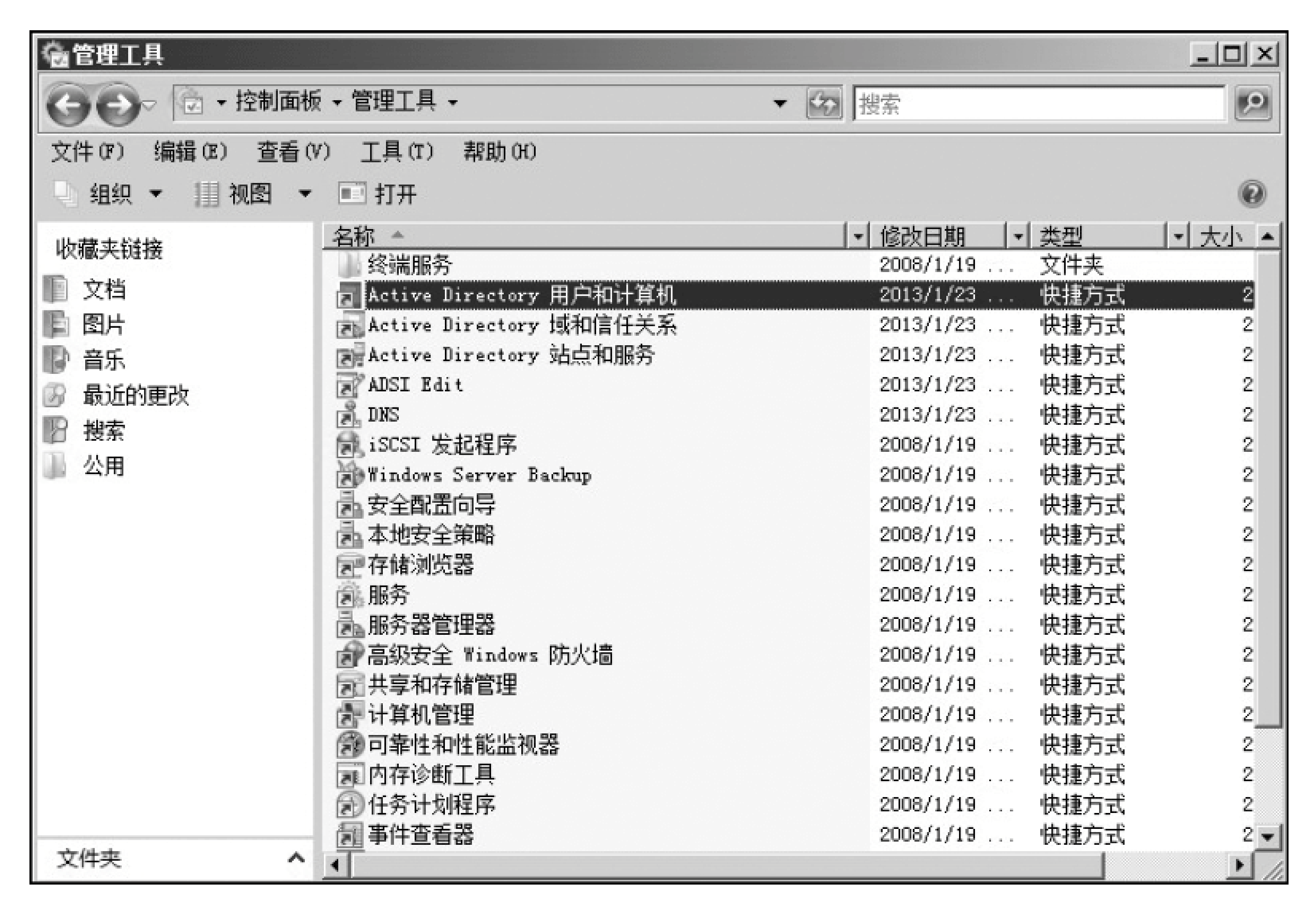


图 2-8 “管理工具”中的新功能图标

如果进入域则选择域选项。作为客户机的本地管理账户，仍然保留对本地计算机进行控制的权力。

(3) 域模式下的默认账户。

在域控制器中，与本地机情况相同，存在着系统创建的默认账户，这些账户有其特定的功能与权限，如图 2-10 所示。

对特殊账户的说明如下：

- Domain Admins（域管理员），用于域范围内的管理，拥有最高权限。
- Administrator（本地（域控制器）管理员），用于域控制器计算机自身的管理。
- Domain（其他默认账户），如图 2-10 所示。



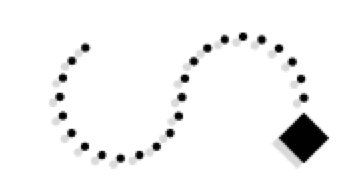
图 2-9 客户机进入域控制器前界面

在基于域模式下的 Windows Server 2008 的账户信息变得异常丰富，域管理员被赋予了极大的权力，对于所有加入域中的用户的账户信息都要进行管理和维护，而账户信息将被域中所有有权获取账户信息的各个部门所使用，从这点可以看出，对域模式下的账户管理涵盖了用户的诸多信息。

注意：建议在设置用户账户密码时不要只是有规律的字母，因为这样极易被网络攻击者猜中，降低了网络的安全防范能力。

3. 域模式下的组概念

在 Windows Server 2008 的域控制器中，组是一个非常重要的概念与应用，账号是进



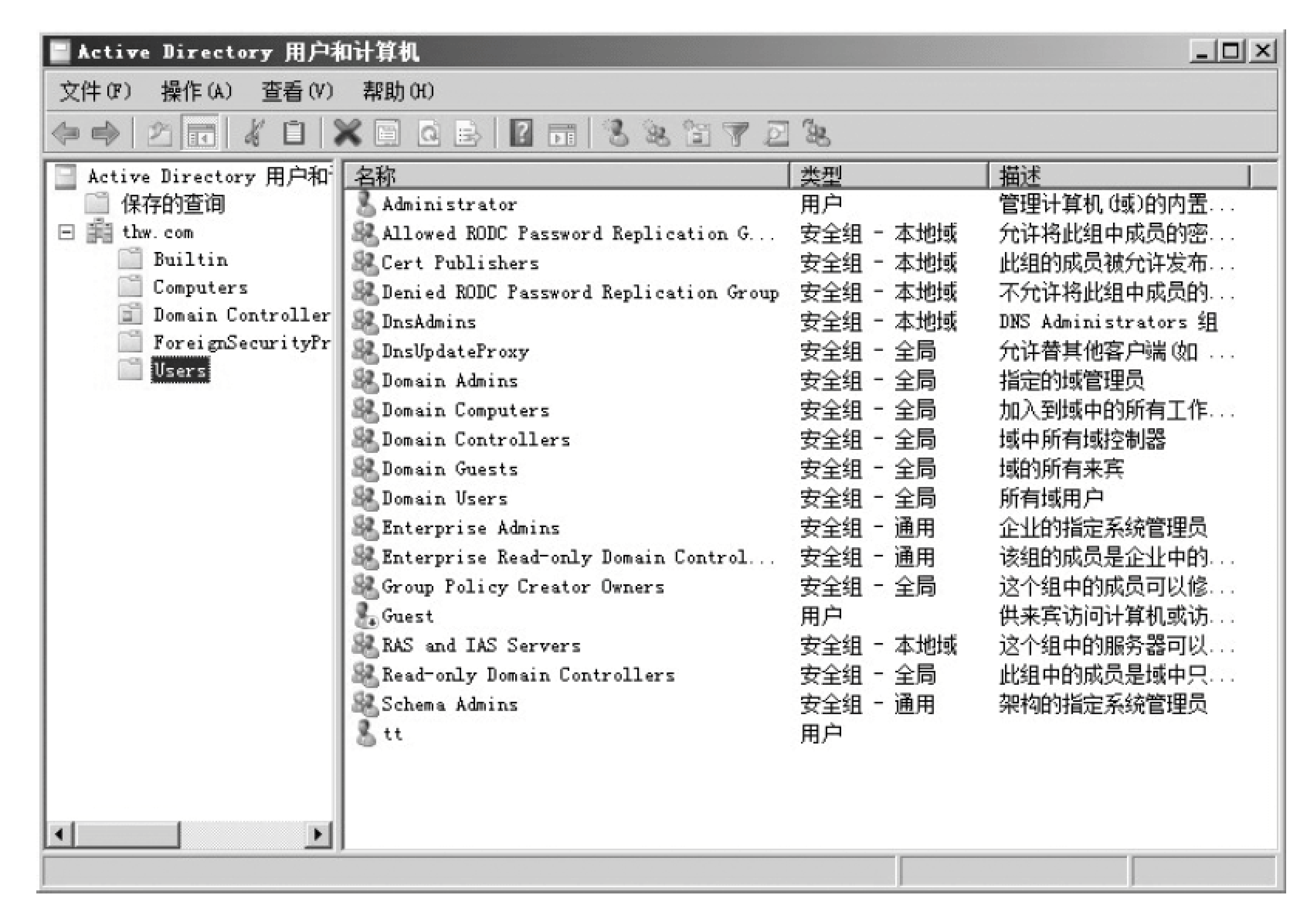


图 2-10　域控制器默认账户

入系统的身份证，组是用来简化、统一管理账户的逻辑结构，利用组可以把具有相同权限需求，相同管理需求的用户组织放置在一个逻辑单元中，进行批量管理，便于管理和提高工作效率。

(1) 组账号的特点。

- 组是个逻辑结构。
- 一个账户可以同时加入多个组。
- 当一个用户加入一个指定组时，该用户账号就拥有了该组所拥有的所有权限。

例如：当我们来到企业进行实习时，每位同学事先准备了不同颜色的帽子，这时领队通知大家，戴红色帽子的同学进左手门，戴黄色帽子的同学进右手门，这时在各个门口守卫的保安并不认识同学，可他会根据每个人所戴帽子的颜色来判别是否允许进入。所以帽子赋予了每位同学相应的权利，帽子就是我们要表示的一种逻辑组。

(2) Windows Server 2008 组的分类。

在 Windows Server 2008 中因组的作用不同，建立了不同类型的组，组有两种类型，即通信组和安全组。

- 通信组：用来组织用户账号，没有安全性，在通信组组中可以存储用户账号等信息，可用于微软的其他相关软件，如 Exchange 2008 Server，如图 2-11 所示。
- 安全组：除了通信组所具备的功能外，主要是用于为用户和计算机设置权限，它是 Windows Server 2008 权限管理的重要组成部分，安全组主要是对所包含的账户在资源对象中的访问控制，如图 2-12 所示。

(3) Windows Server 2008 组的范围。

组的范围是用来管理组的作用域的，在域中根据组的范围进行分类，有三种类型，即全局组、本地组和通用组。

图 2-11 通信组



图 2-12 安全组

• 全局组：用来管理具有相同管理任务的用户账号，在该组中只能包括该组所在域的用户账户，该组可成为域的本地组成员。

• 本地组：与全局组不同，本地组的目的是为了给本域中的资源分配权限，本地组只在本域中可见。该组可以包括任何域的用户账号和任何域的全局组和通用组。

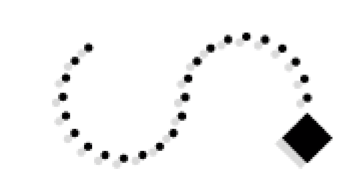
• 通用组：具备了以上两个组的作用，其成员灵活，其作用主要是在多域模式下组织全局组。

（4）Windows Server 2008 中的默认组。

在一个域搭建好后，打开“Active Directory 用户和计算机”工具中的 Users 文件夹，就出现了一些已经存在的账户和组，如图 2-13 所示。



图 2-13 已存在的账户和组



在这些组中,可以分成 4 类:预定义组、内置组、内置本地组和特殊组。

① 预定义组:这些组创建在 Users 文件夹中,默认情况下为全局组,没有任何继承权力。

例如:Domain Admins(域管理员组),自动将该组加入 Administrators,具有域的管理权限。

Domain Guests(域来宾组),具体解释说明见文件夹中的"描述部分"。

Domain Users(域用户组),自动加入本地 Users 组中,成为域中用户组成员。

② 内置组:在 Builtin 文件夹中建立的组为内置组,如图 2-14 所示。

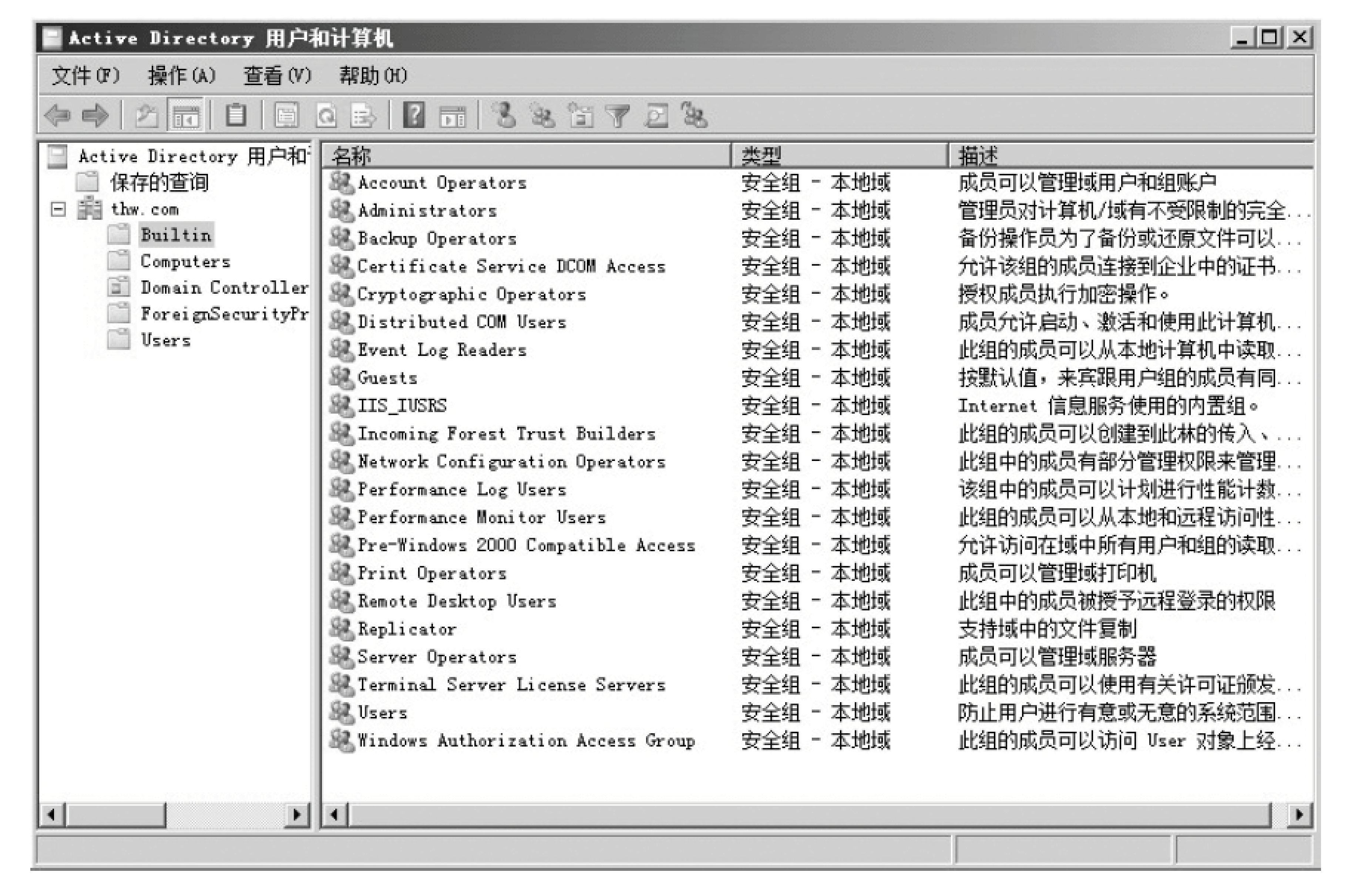


图 2-14　内置组

这些组都是安全本地组,提供预定义用户权力和权限的管理,这些组已经设置好相应的权限,如果让那些用户执行相应的管理权限,只要把这个用户账号加入对应组中即可。

Account Operators(用户账户操作员组):成员可以管理域用户和组账户,但不能修改 Administrators 组的任何信息。

Administrators(管理员组):管理员对计算机/域有不受限制的完全访问权。

Backup Operators(备份操作员组):备份操作员为了备份或还原文件可以替代安全限制。

Users(备份操作员组):用户无法进行有意或无意的改动。因此,用户可以运行经过验证的应用程序,但不可以运行大多数旧版应用程序。

③ 内置本地组:该组不属于活动目录域模式下的组,前面已经讲述。

④ 特殊组:该组没有特定的用户账户,但可以在不同时候代表不同用户,例如:Everyone(每人组)。

2.1.2　组织单位

网络操作系统在日常的管理中有着丰富和复杂的内容,例如:对账户使用计算机的

系统配置的管理，对网络环境的管理，对桌面设置的管理，对安全设置的管理等。在这样的需求下，如果管理员对每个用户账户都一一进行设置，那将是天文数字的工作量。因此，应当通过一个适当的方法简化这些重复性工作。这就要求我们分析企业对员工进行的管理活动。在企业的日常管理往往是按照部门进行管理的，一个部门员工具有相同的工作环境、工作要求、相同的权利，这样就可以把员工的所有需求设置在一个属于部门的管理制度或管理方法中，当一个员工加入了该部门时，则所有的要求均依照部门要求执行。

在活动目录的域模式中，提供了一个重要的概念与之对应，它就是 OU。OU 是非常重要的一个组件，在资源组织和管理上起着重要的作用，它可以将被管理的对象统一放置在一个逻辑机构内，这些对象包括用户账号、组账号、计算机、打印机、共享文件夹以及子 OU。当这些对象被放置在 OU 容器后，围绕着这个 OU 就可以进行一系列的管理设置了。

在 Active Directory 活动目录中的 OU 对象，使得整个域的规划与管理更有弹性，更能发挥“分层负责，授权自治”的优点。或者说，OU 就是一个比域要小的管理单元，如果善用 OU，就可以避免形成多域的复杂架构。OU 纯粹是一个逻辑概念，它可以帮助我们简化管理工作。OU 可以包含各种对象，通过使用域模式 OU 管理体系可以使得管理变得简捷高效。

(1) OU(组织单元)与组账号的区别。

OU 与组账号都是域模式下的管理对象，OU 管理的对象更多些，而组账号只对用户账户在文件夹上的权限进行管理。

当删除组账号时，组账号所管理的用户账号的逻辑关系就被打破、消失，而用户账户本身不会消失。但删除了 OU，在 OU 中设置的信息、加入管理的对象将随之删除。

(2) OU 与域的关联。

域是安全的边界，域是操作系统对所有与之连接的计算机和登录计算机的用户账户的全面的管理，是建立在活动目录中的最全面完善的网络管理模式，用户访问计算机时需先登录域再进入 OU。

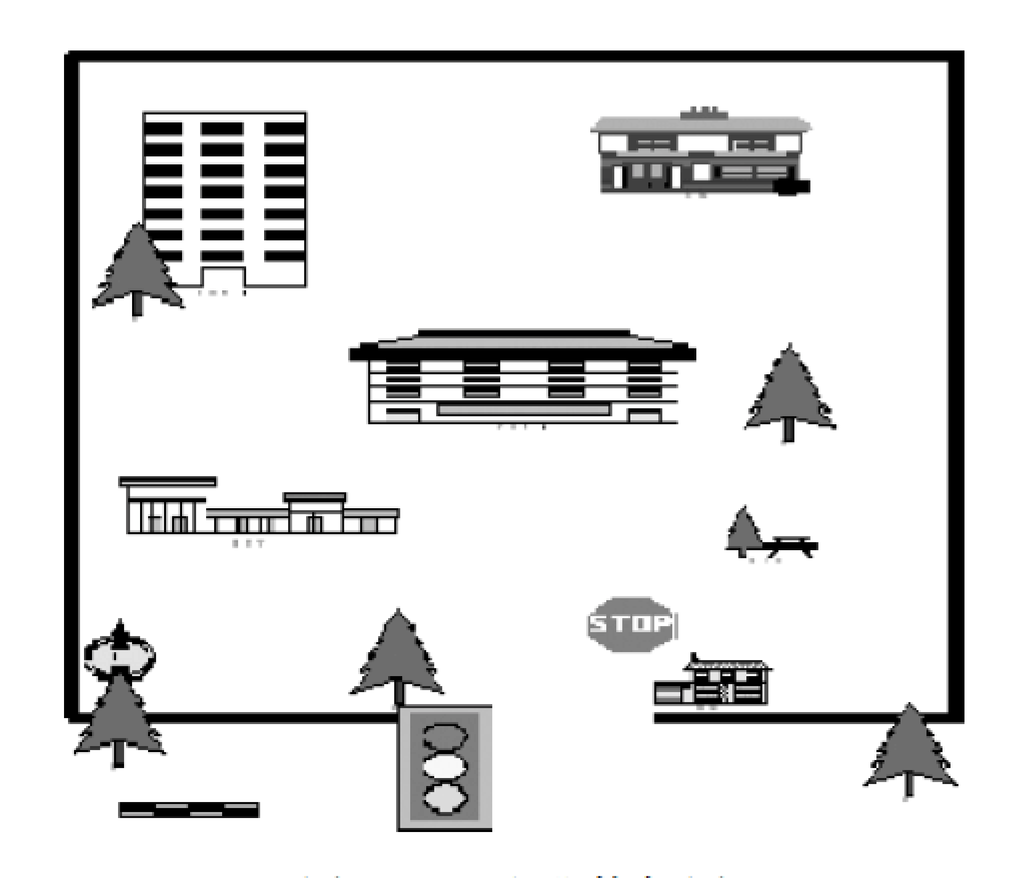
OU 在域模式中存在一个具体的逻辑管理方式且依存于域。

例如：一个企业，由各种环境、各种设备、各类人、各项工作构成，在这个企业周边筑起围墙，这个围墙就是域，围墙内的一切受到了保护，围墙内的一切都有着自己的天地且相互协调相互帮助，围墙外面的一切受到限制，要想进入企业必须通过安检和授权，如图 2-15 所示。

在这个企业中每个人都有自己的分工，都有自己的职权范围，最重要的是每位员工都归属到一个部门，因为企业的管理模式、工作类别、权力范围都有着对不同类别工作的规范性要求，因此建立各个专业部门，一般情况下有技术、人事、财务等部门，如图 2-16 所示。

在一个部门有一定的员工，有该部门专用的设备、自己独特管理方式，有统一的着装、特殊的办公环境，以及独特的安全管理规定。

通过这些我们看出一个企业内部众多的员工，被归属到各个部门，各个部门又有自己相对独立的管理方式。而这些独立的部门就是我们所讲的 OU(组织单元)，各个部门的独立的管理规范就是我们将要在后面讲述的组策略。



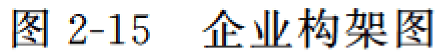


图 2-15　企业构架图

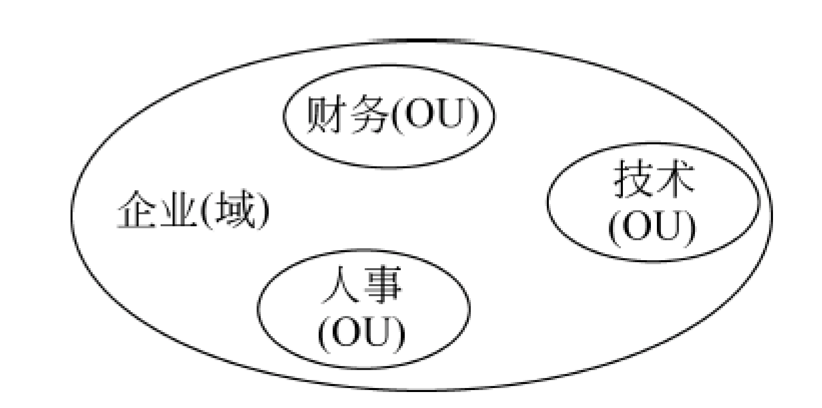


图 2-16　企业机构示意图

2.2　域和子域的建立

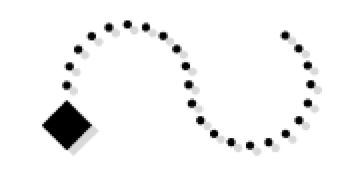
2.2.1　Active Directory 创建域控制器

Windows Server 2008 系统的 Active Directory（活动目录）服务和以前的版本相比，其不同之处是：可以通过“服务器管理”的角色添加来完成初始化的准备工作。

（1）选择“开始”→“管理工具”→“服务器管理器”命令，显示“服务器管理器”窗口，单击“服务器管理器”左侧列表中的“角色”选项，如图 2-17 所示。



图 2-17　服务器管理器



(2) 启动添加角色向导。

在"服务器角色"列表中勾选"Active Directory 域服务",如图 2-18 所示,此时,系统会自动弹出对话框。

图 2-18　选择服务器角色

要求安装".NET Framework 3.5.1 功能",因为 Active Directory 在 Windows Server 2008 上必须有该功能的支持,如图 2-19 所示。

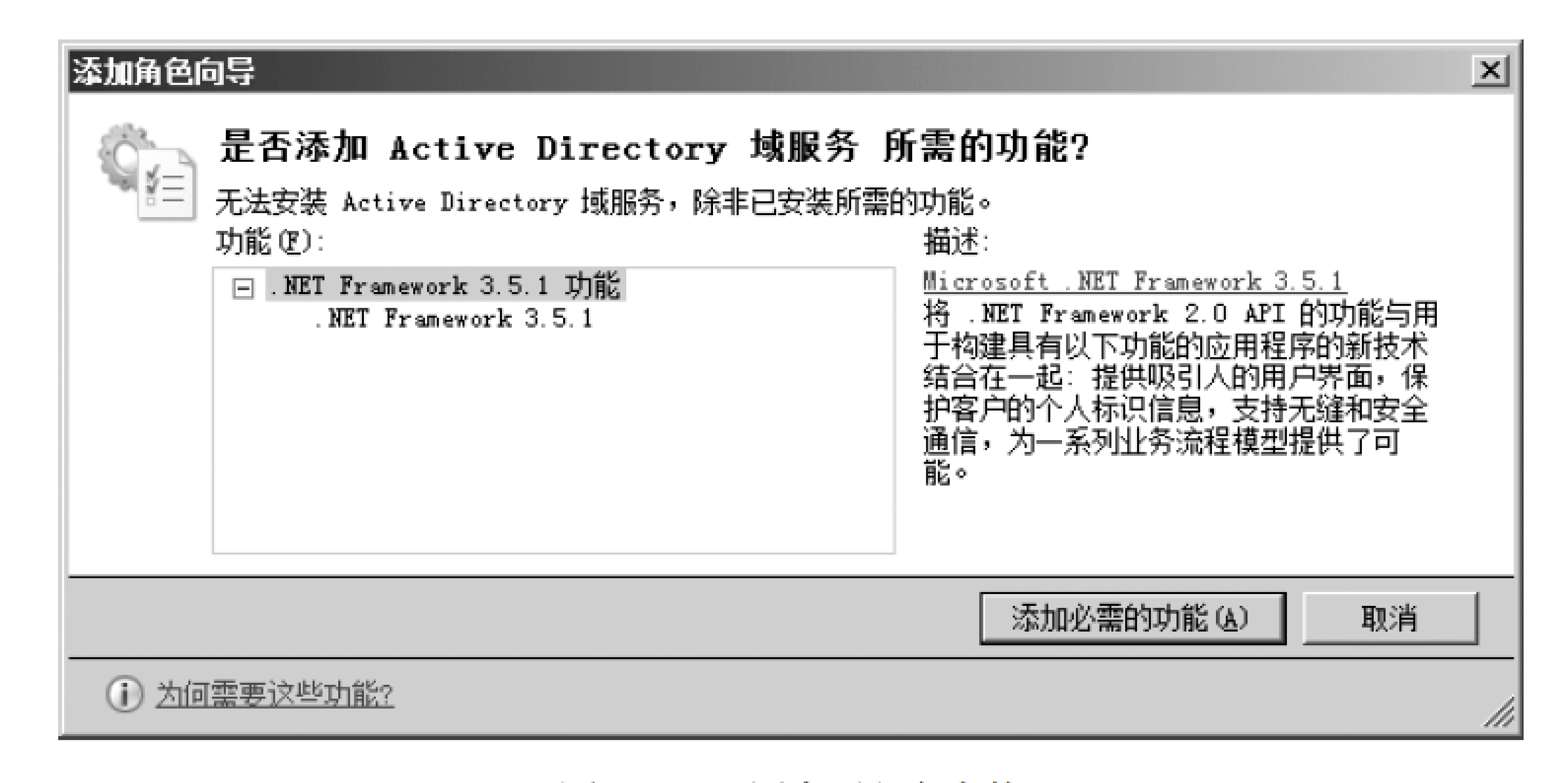
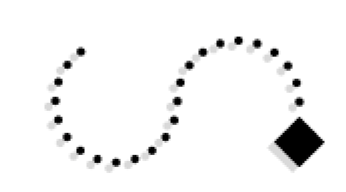


图 2-19　添加所需功能

所以在此必须单击"添加必需的功能"按钮,返回"选择服务器角色"对话框后单击"下一步",然后按安装向导的提示进行"下一步"的安装,如图 2-20 所示。

当出现"安装结果"对话框时,如果没有错误,就证明 Active Directory 的安装准备已经完成,但是由于该台计算机还不能完全正常运行 DC,所以提示需要启用 Active



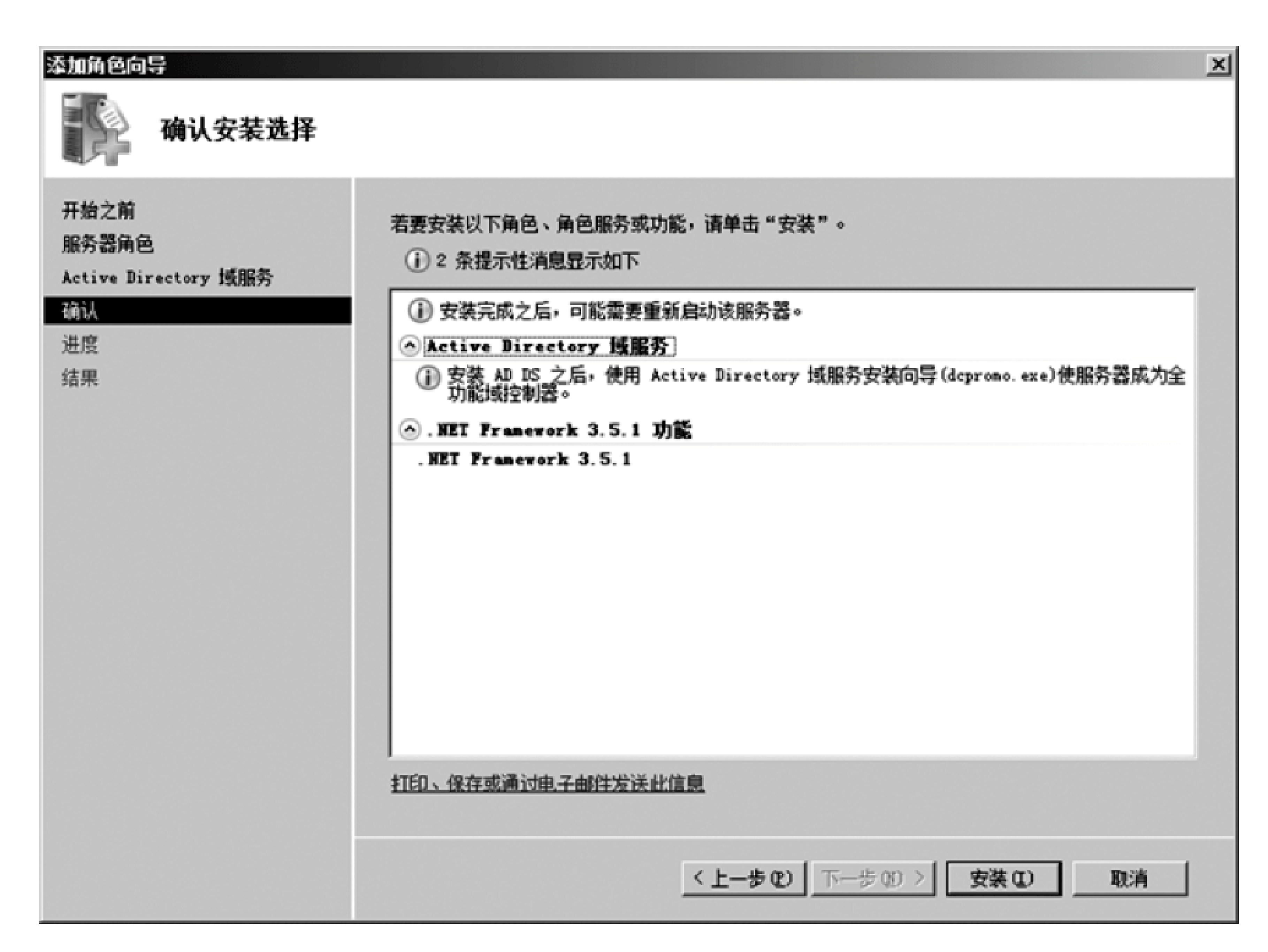


图 2-20　确认安装选择

Directory 安装向导(dcpromo.exe)来完成安装，如图 2-21 所示。可以直接单击“关闭该向导并启动 Active Directory 域服务安装向导(dcpromo.exe)”进入安装向导，也可以直接单击“关闭”按钮之后，手动打开 Active Directory 安装向导。

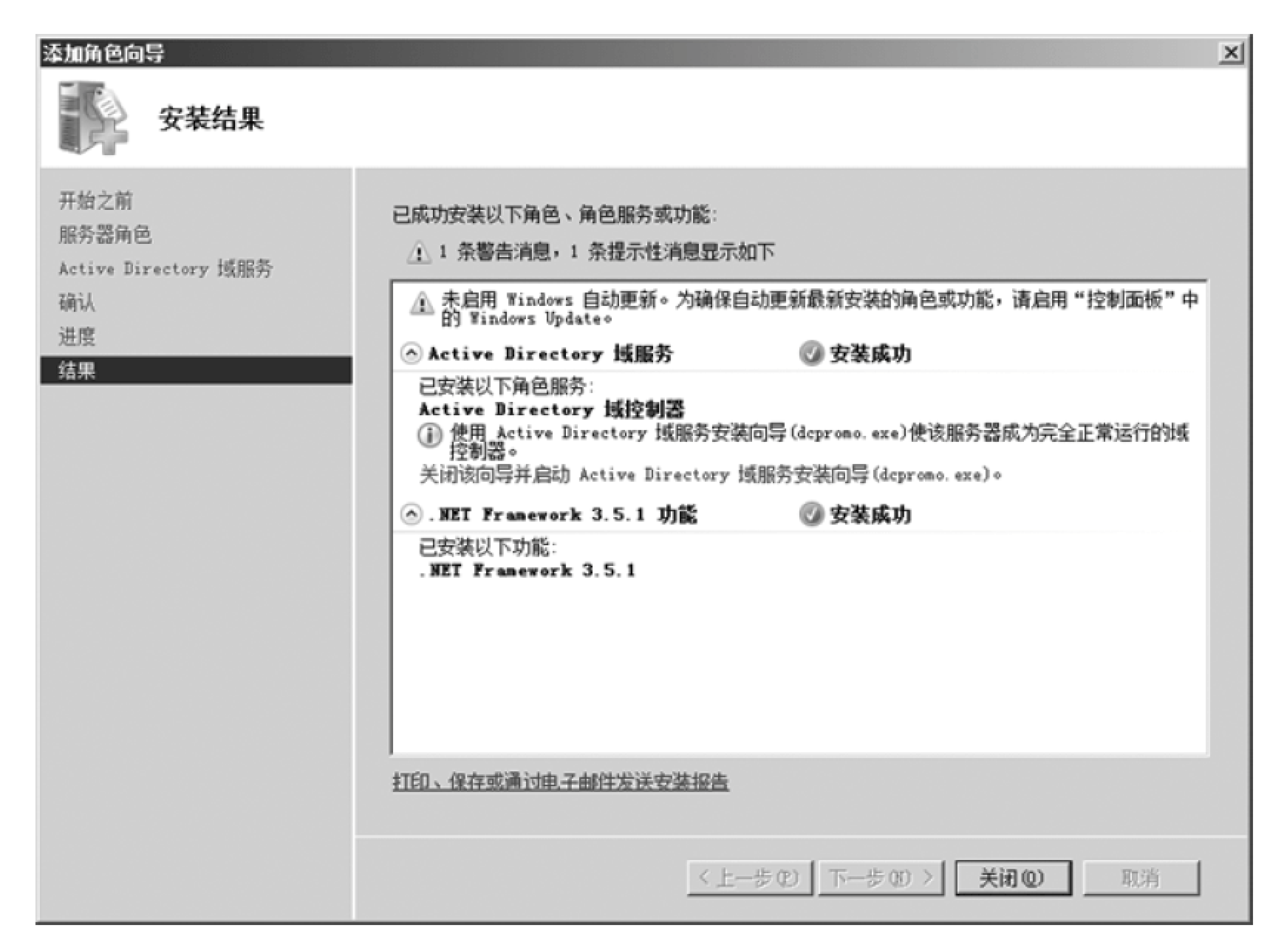


图 2-21　安装角色结果

（3）运行 dcpromo 命令安装活动目录服务。

在网络服务器上安装 Windows Server 2008 操作系统后，使用 dcpromo 命令启动活动目录的安装向导，如图 2-22 所示。

单击“确定”后，启动“Active Directory 域服务安装向导”，单击“下一步”，如图 2-23 所示。

（4）弹出“操作系统兼容性”对话框，单击“下一步”按钮，如图 2-24 所示。

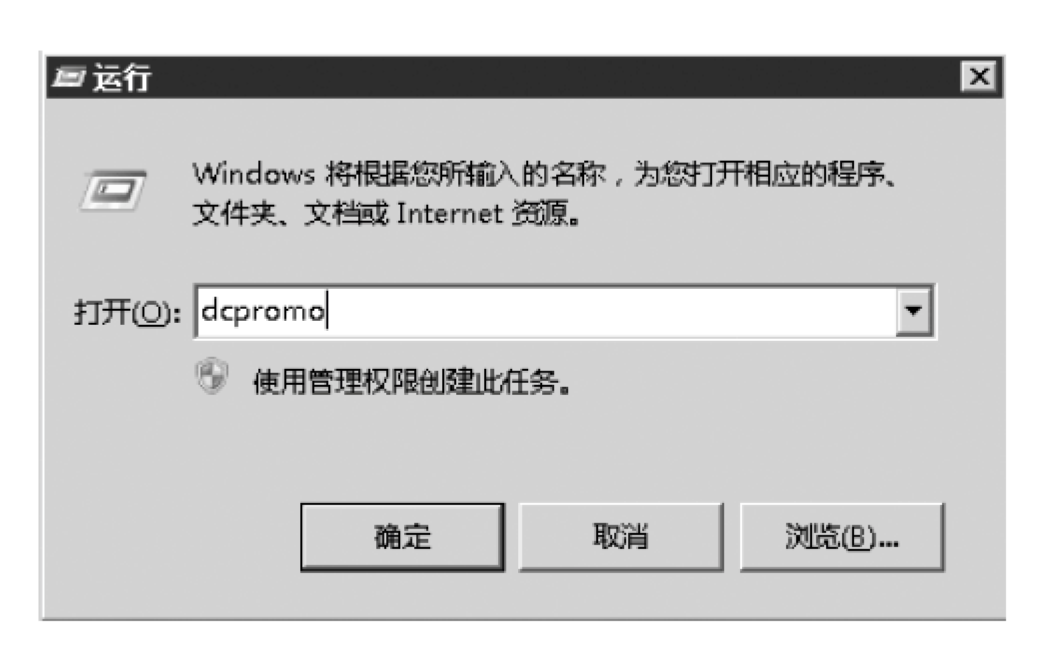


图 2-22　运行 dcpromo 命令

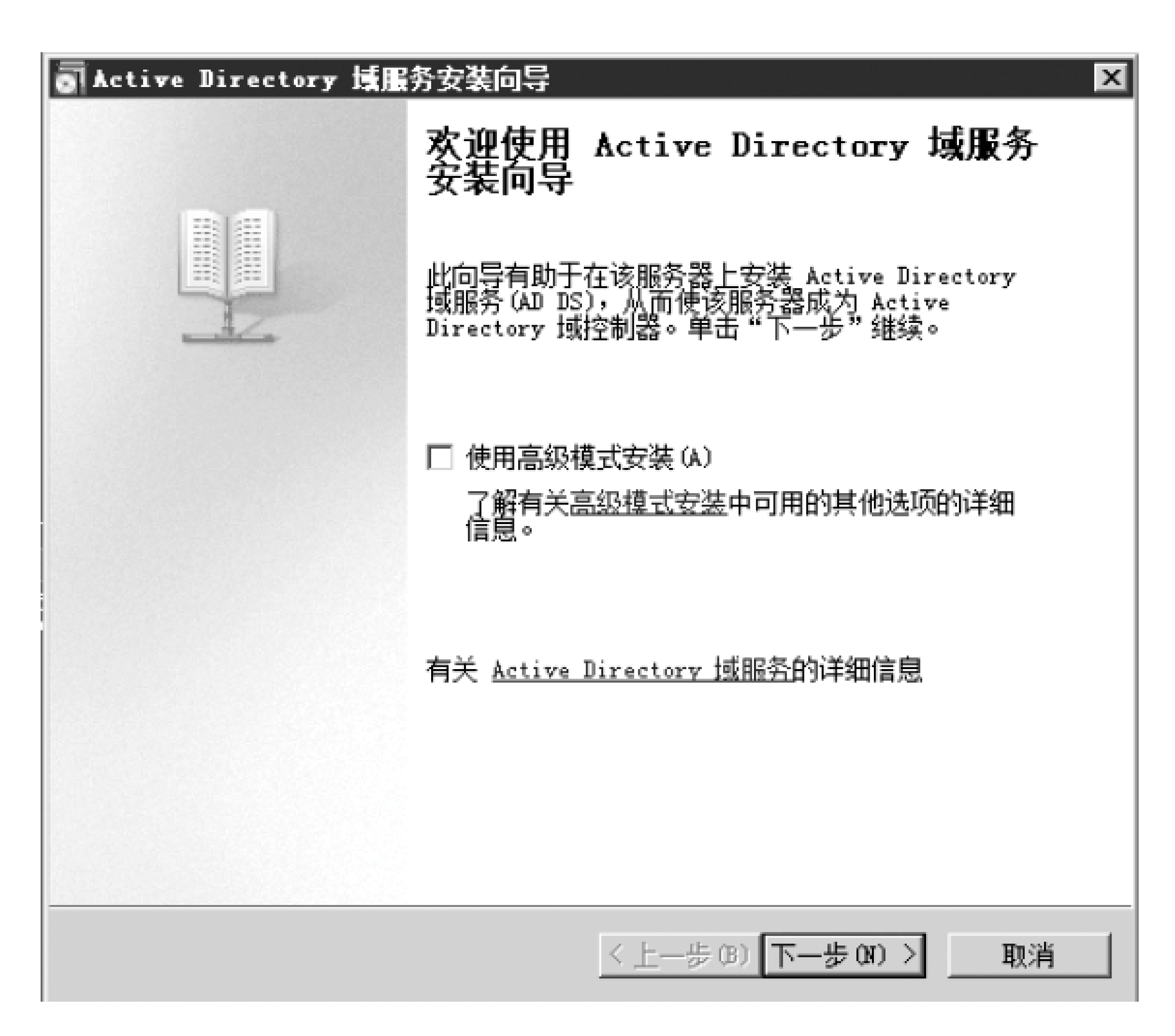


图 2-23　启动 Active Directory 域服务安装向导

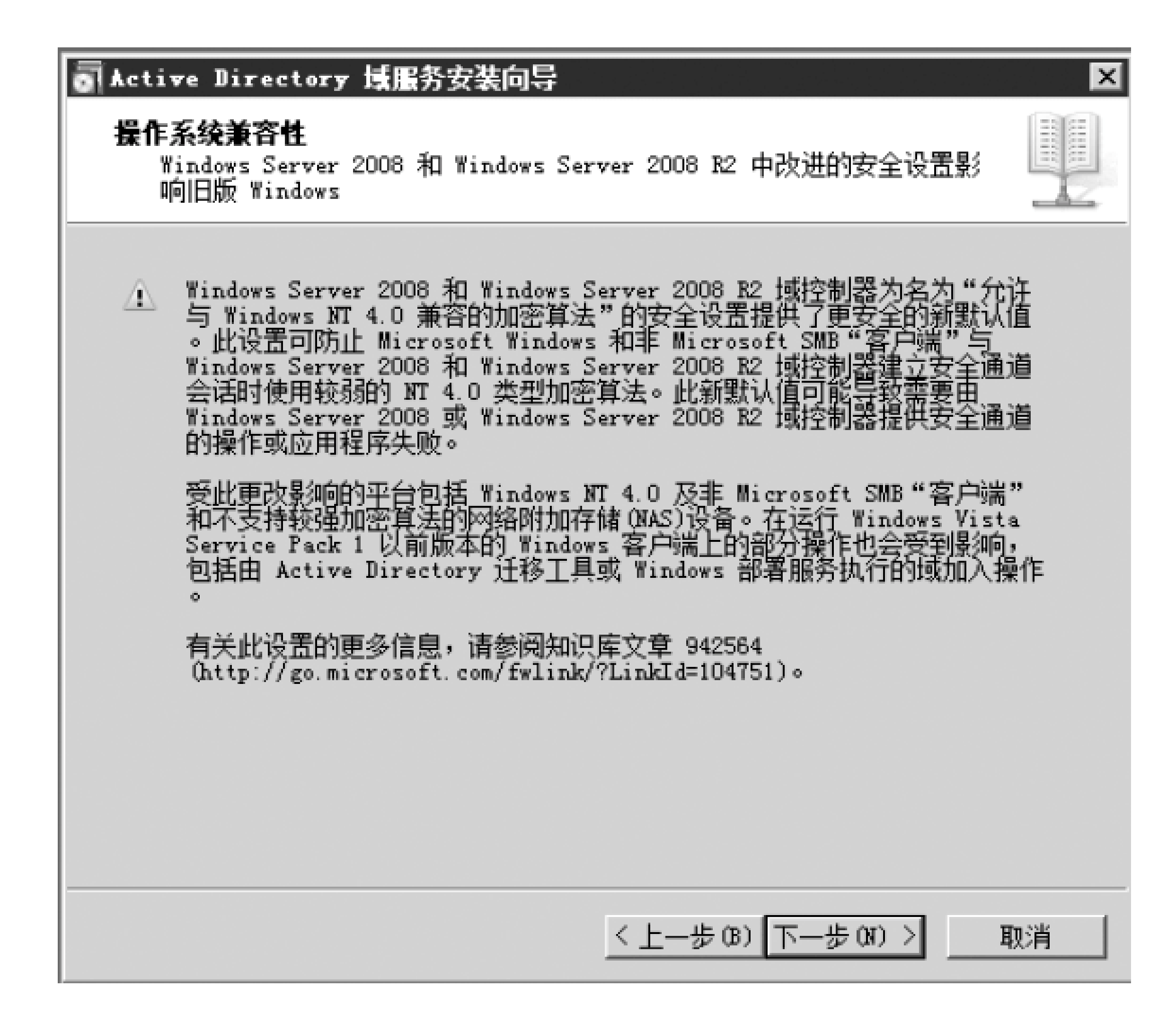


图 2-24　操作系统兼容性

（5）进入“选择某一部署配置”对话框，安装向导提供 Active Directory 安装模式，包括在现有 Active Directory 中添加域控制器（现有林）和全新的 Active Directory（在新林中新建域）两种，这里我们选择后者，在新林中新建域来全新安装 Active Directory，如图 2-25 所示。

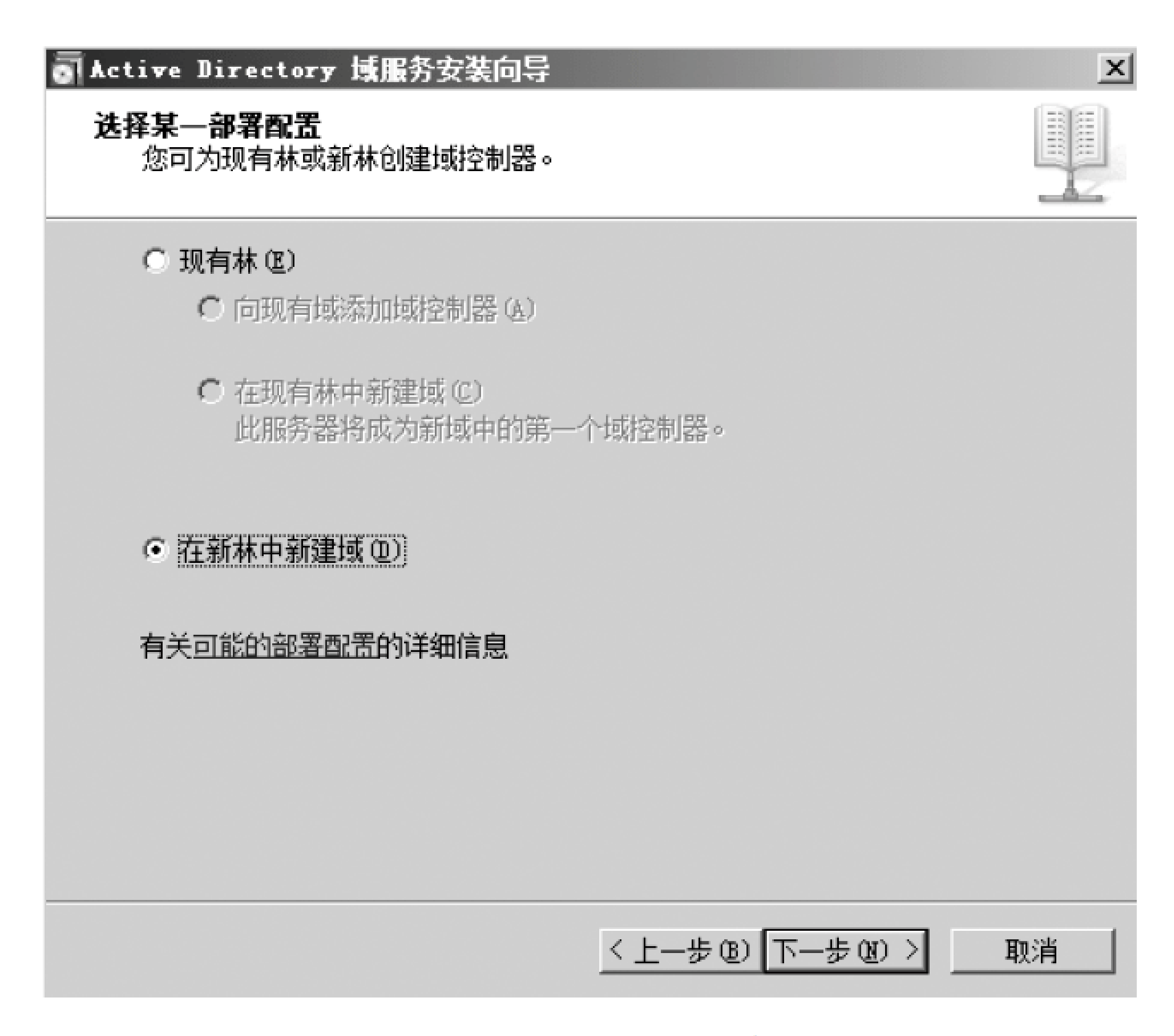


图 2-25　在新林中新建域

（6）然后单击“下一步”按钮，显示“命名林根域”对话框，在“目录林根级域的 FQDN”文本框中输入新根域的名称 abc.com，如图 2-26 所示。

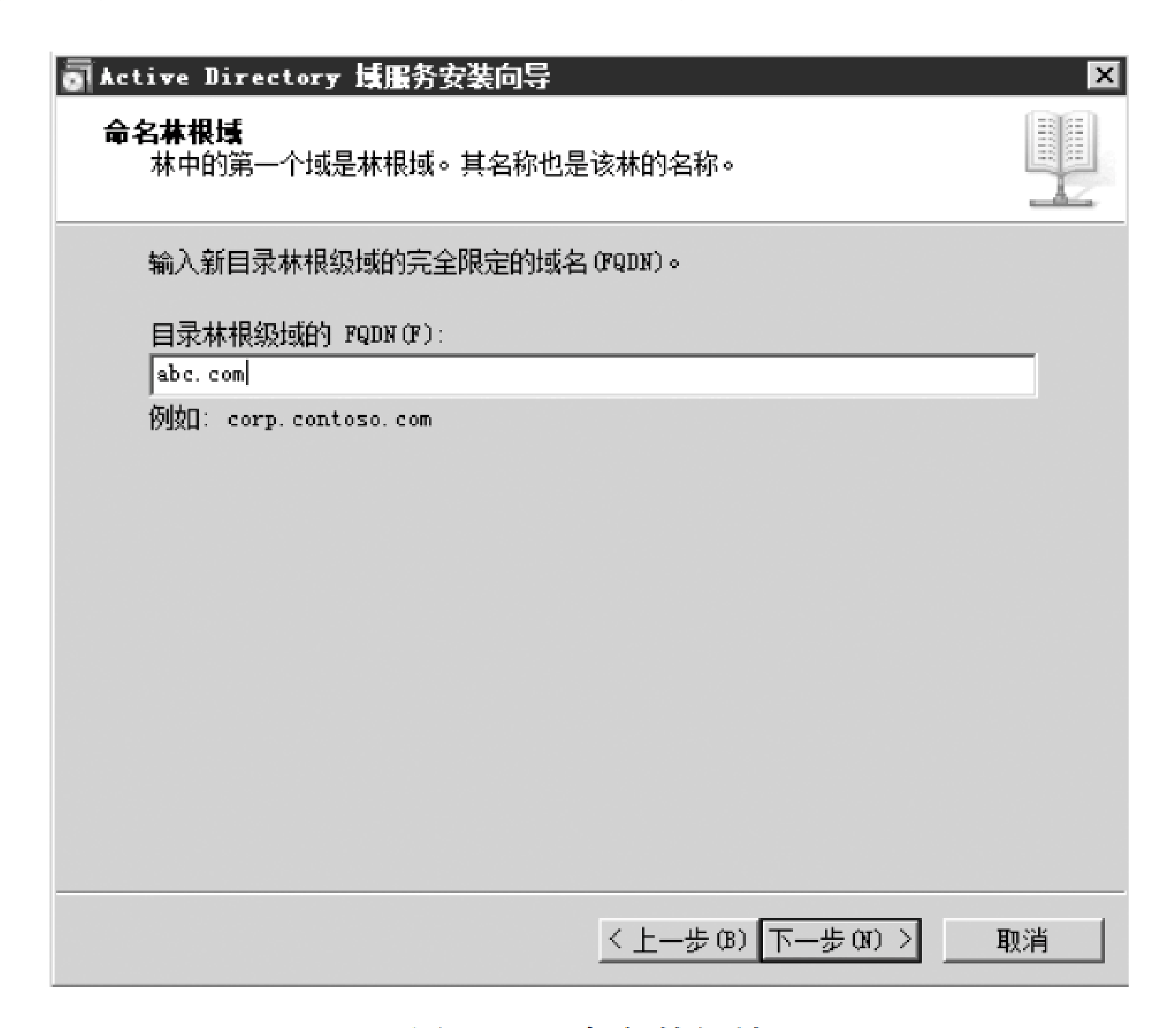


图 2-26　命名林根域

（7）单击“下一步”按钮，显示“设置林功能级别”对话框，在“林功能级别”下拉列表框中选择欲使用的安装模式，如图 2-27 所示。



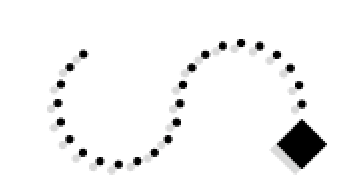
图 2-27　设置林功能级别

（8）单击“下一步”显示“其他域控制器选项”对话框。默认在林根服务器安装 DNS 服务器，如果网络中使用单独的 DNS 服务器，可以取消选中“DNS 服务器”复选框，如图 2-28 所示。



图 2-28　其他域控制器选项

（9）单击“下一步”，这时系统会检查本系统是否是静态 IP 地址，查找 DNS 的父区域。我们使用静态 IP 地址，如图 2-29 和图 2-30 所示。



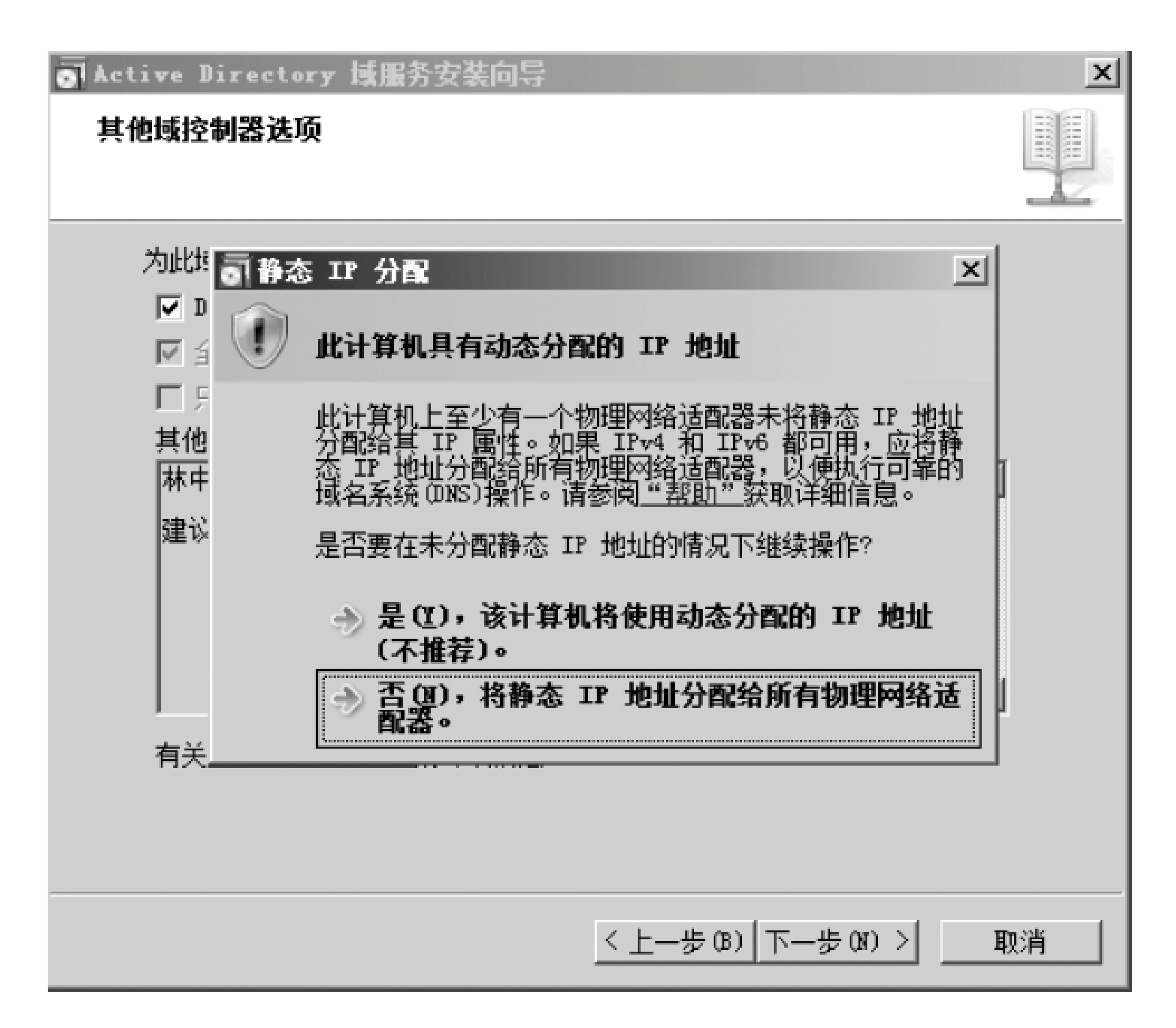


图 2-29　安装 DNS 服务器 IP 地址检测

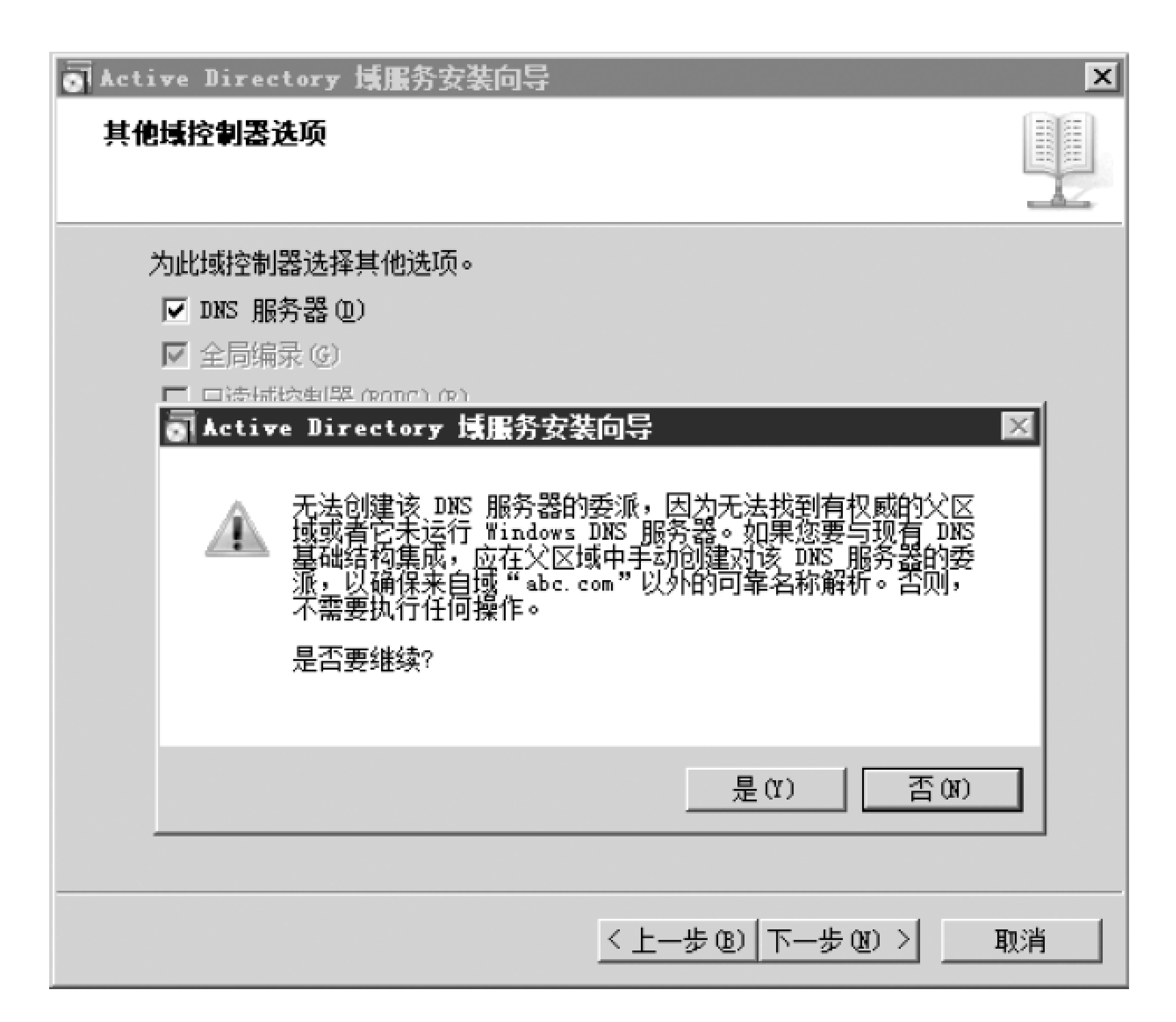


图 2-30　DNS 父区域检测

注意：由于默认在林根服务器安装 DNS 服务器，因此在这里使用的本主域控制器的 IP 地址为 DNS 地址。

(10) 单击"是"，继续"下一步"显示"数据库、日志文件和 SYSVOL 的位置"对话框，建议将这三个文件夹都分开存储在不同的物理磁盘中，这样可以保证数据安全，提高 Active Directory 的性能，如图 2-31 所示。

(11) 单击"下一步"按钮，显示"目录服务还原模式的 Administrator 密码"对话框，密码建议要符合强密码策略要求，如图 2-32 所示。

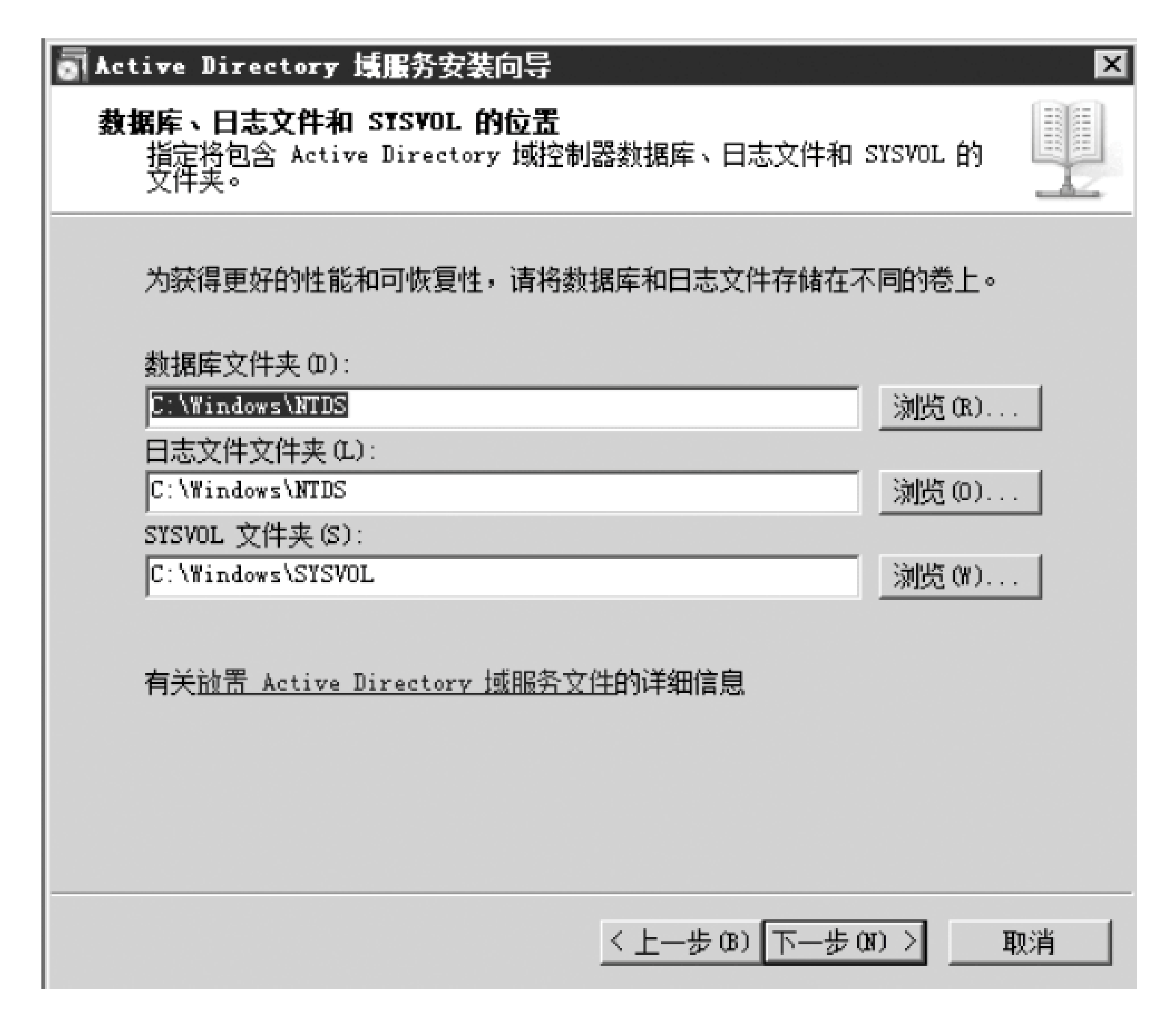


图 2-31　确定数据库、日志文件和 SYSVOL 的位置

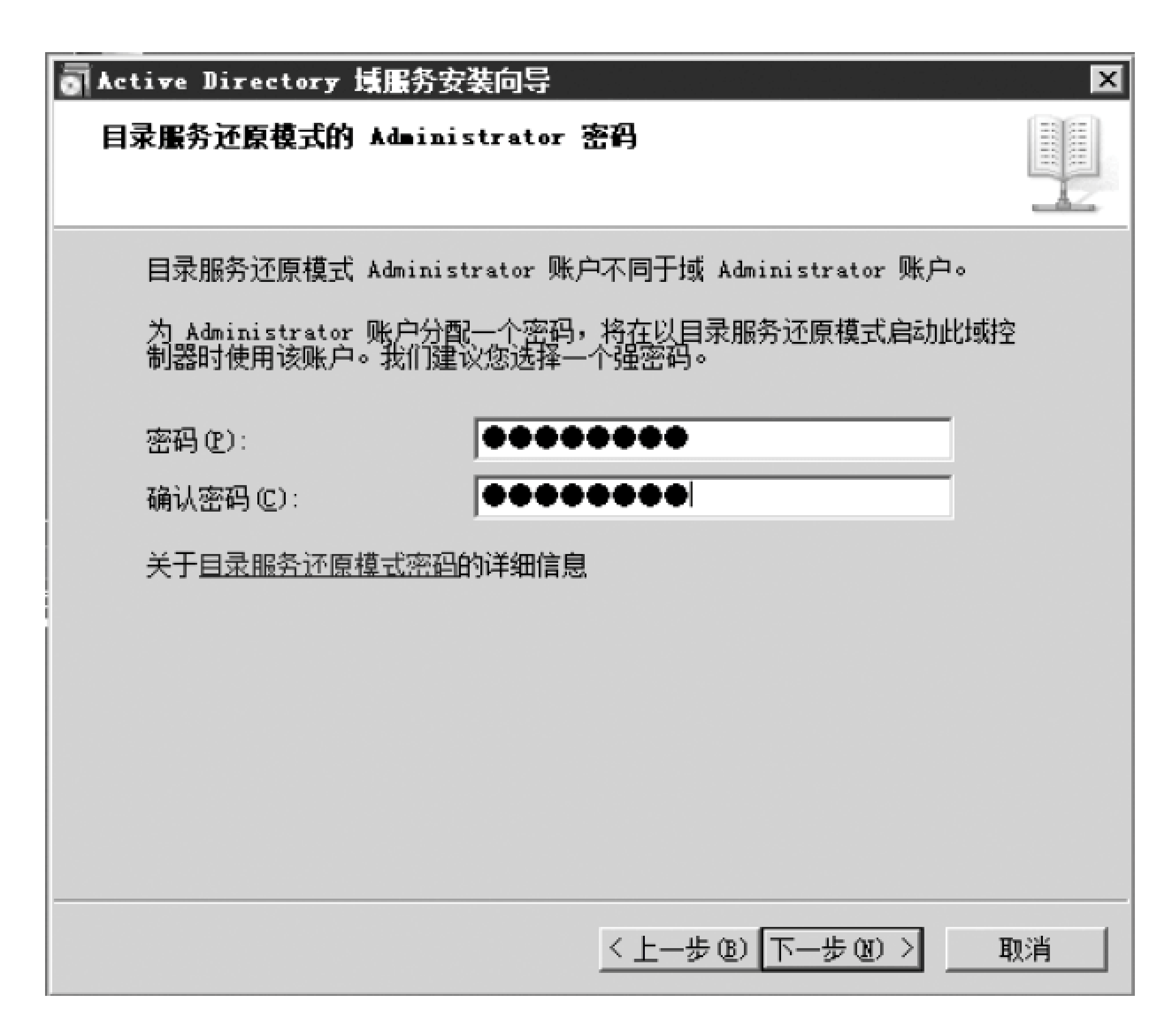


图 2-32　为目录服务还原模式设置 Administrator 密码

(12) 单击“下一步”显示“摘要”对话框，显示 Active Directory 设置信息，可以使用“导出设置”按钮导出并保存成文本文件，如图 2-33 所示。

(13) 单击“下一步”按钮，开始安装 Active Directory，如果选择“完成后重新启动”复选框，可以在完成安装后自动重新启动计算机，如图 2-34 所示。

(14) 安装完成，显示“完成 Active Directory 域服务安装向导”对话框。单击“完成”按钮，关闭安装向导，重新启动计算机后，活动目录(Active Directory)安装成功，如图 2-35 所示。

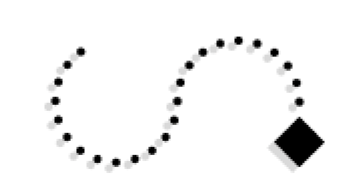




图 2-33　摘要

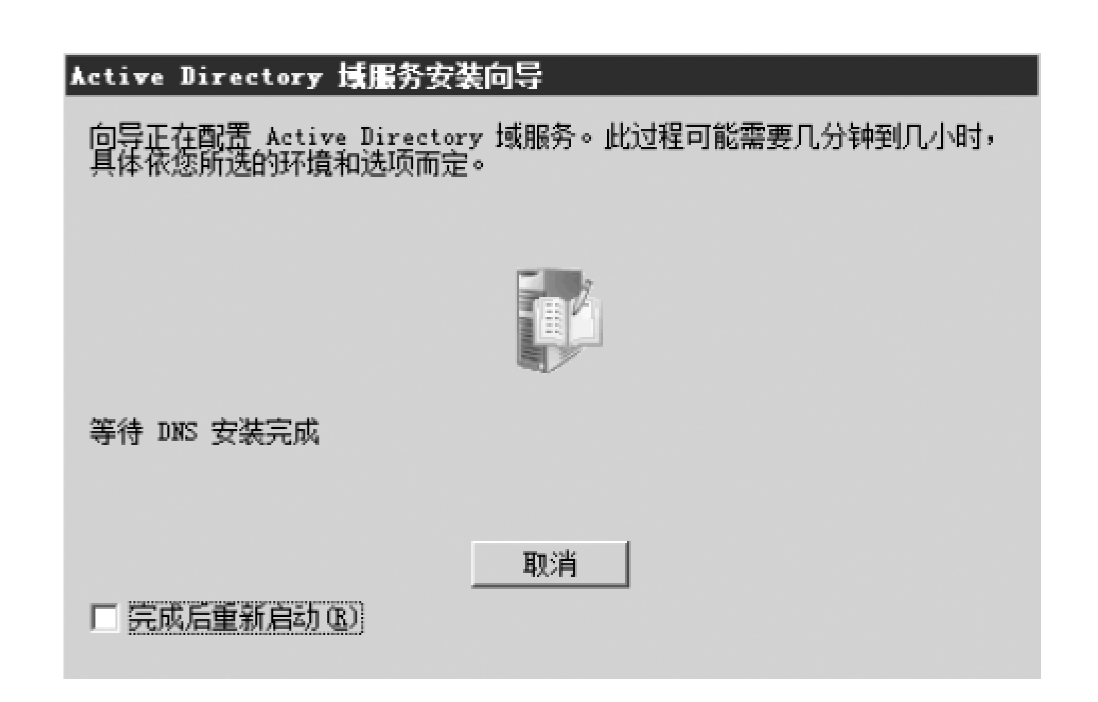


图 2-34　正在配置活动目录

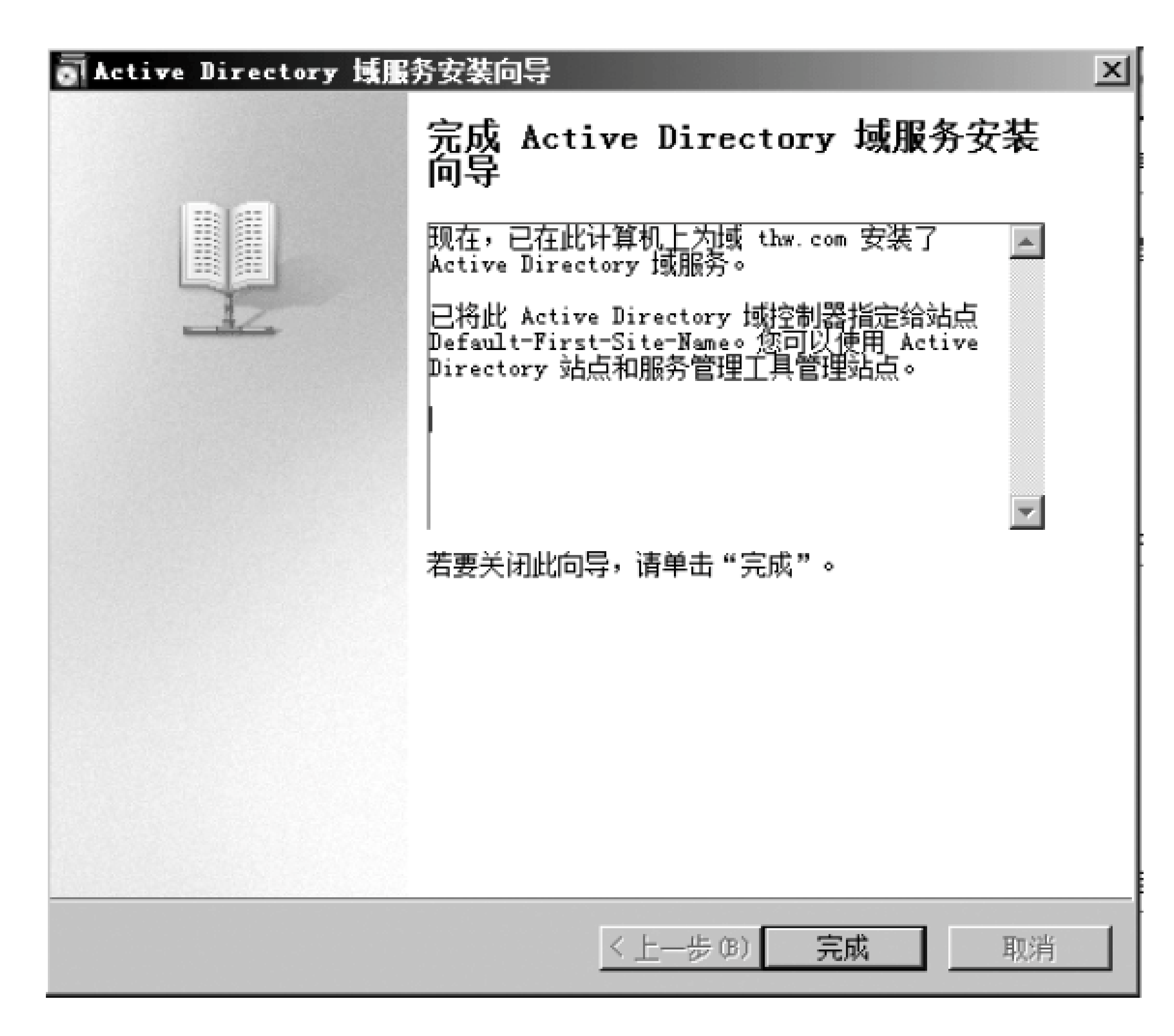


图 2-35　完成活动目录域服务器的安装

2.2.2 创建子域控制器

前面已经讲了如何新建域控制器，现在我们讲解如何建立子域。首先，保证主域控制器是开启状态，然后我们再打开一台工作组计算机，做以下配置工作。

IP 地址：192.168.1.2。

子网掩码：255.255.255.0。

DNS 地址：192.168.1.1(写主域控制器的 IP 地址)。

(1) 单击“开始”→“运行”，输入 dcpromo，出现了“Active Directory 域服务安装向导”对话框，如图 2-36 所示。

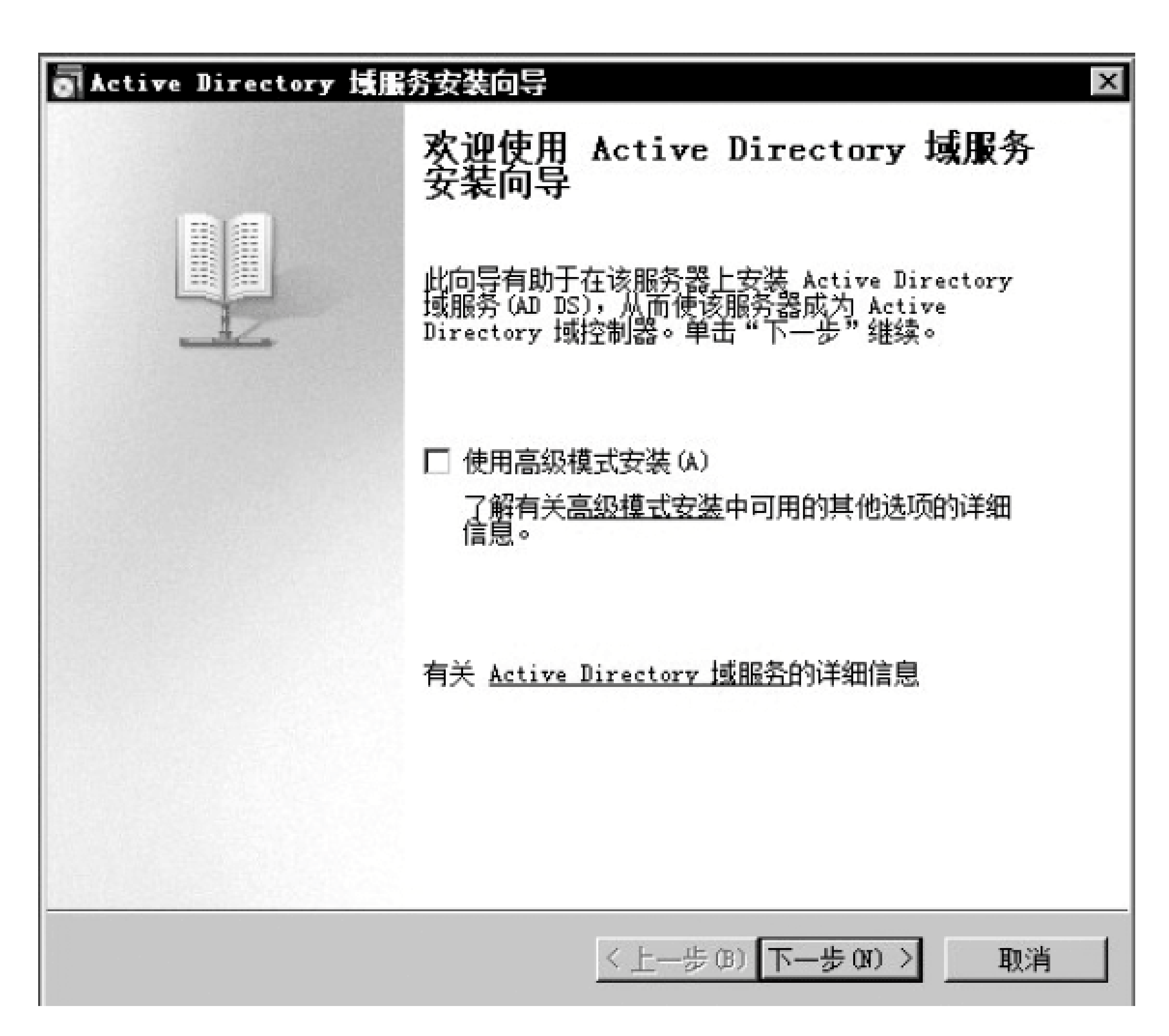


图 2-36　域服务器安装向导

(2) 单击“下一步”出现“选择某一部署配置”对话框，我们选择“现有林”，因为我们现在是做子域，是一个新的域控制器但是要建立在现有的林中，所以选择“在现有林中新建域”，如图 2-37 所示。

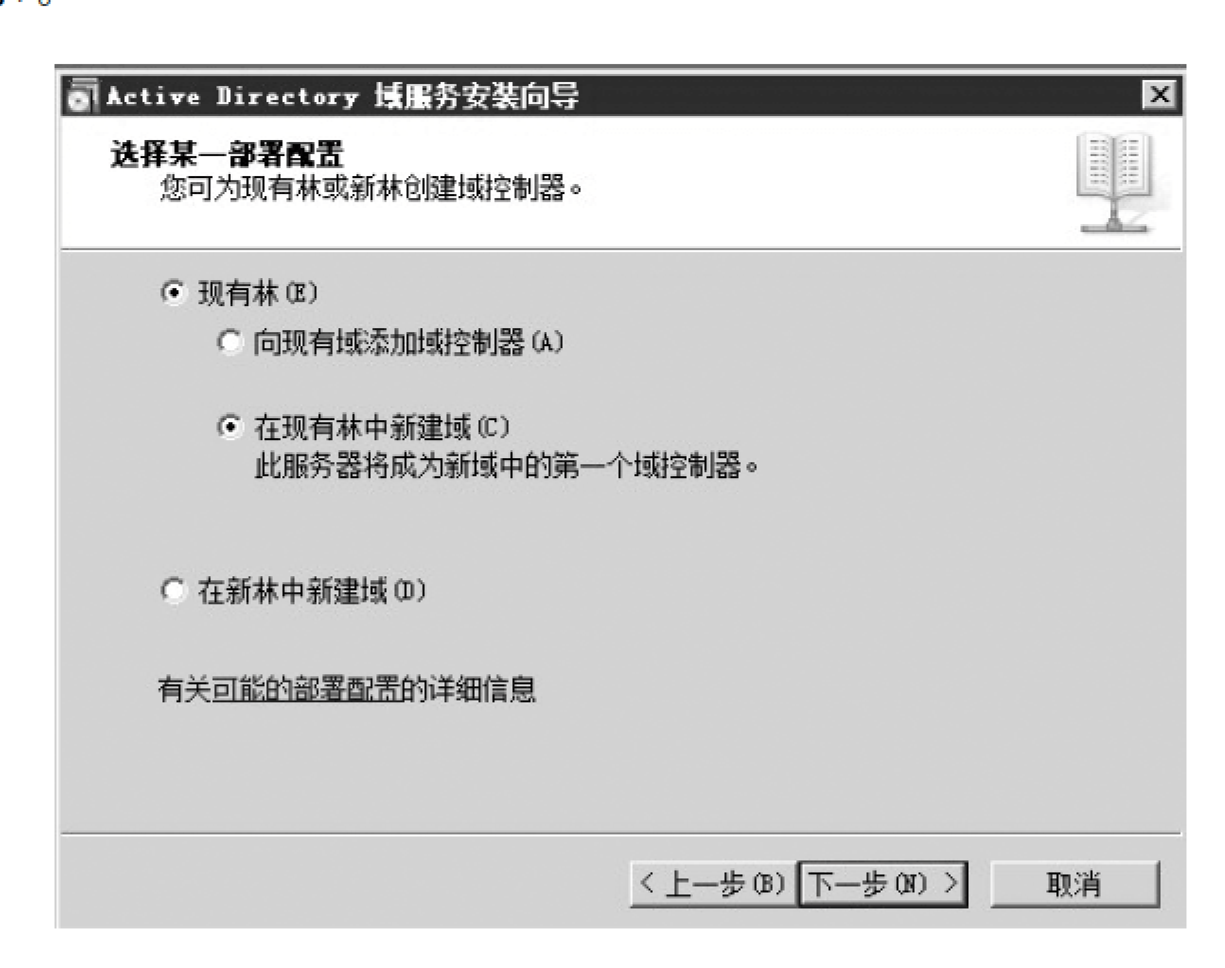
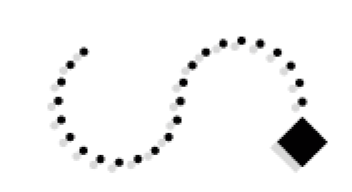


图 2-37　选择在现有林中新建域



（3）这里我们输入父域中主域控制器的管理员和密码(在第一个案例中我们建立的主域)，域里写父域的域名 abc.com，在输入凭证对话框中输入主域控制器的用户名及其密码，如图 2-38 所示。



图 2-38　网络凭证

（4）单击“确定”并与父域建立了联系后，会出现“命名新域”对话框，在“父域的 FQDN”文本框中写父域的 DNS 全名 abc.com ，子域里写 sub 就可以了，我们可以在“新域子域的 FQDN”中看到显示出 sub.abc.com，这个就是我们要建立的子域，如图 2-39 所示。

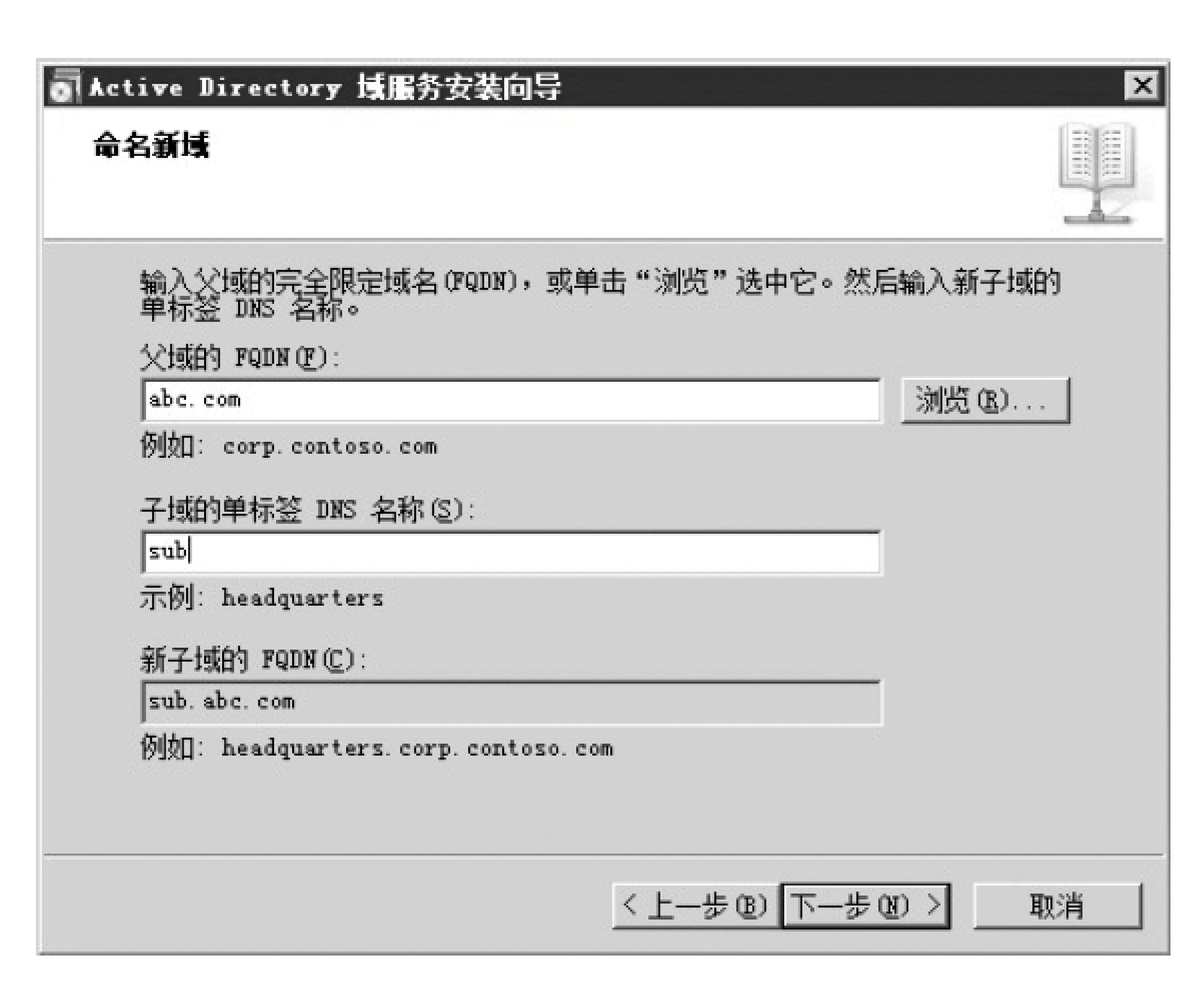


图 2-39　输入要建立的子域名字

（5）单击"下一步"，系统开始验证域名，如图 2-40 所示。



图 2-40　验证域名

（6）当系统验证域名通过后，出现"域 NetBIOS 名称"对话框，如图 2-41 所示。我们在"域 NetBIOS 名称"文本框中输入子域中域控制器的 NetBIOS 名——ASUKA。

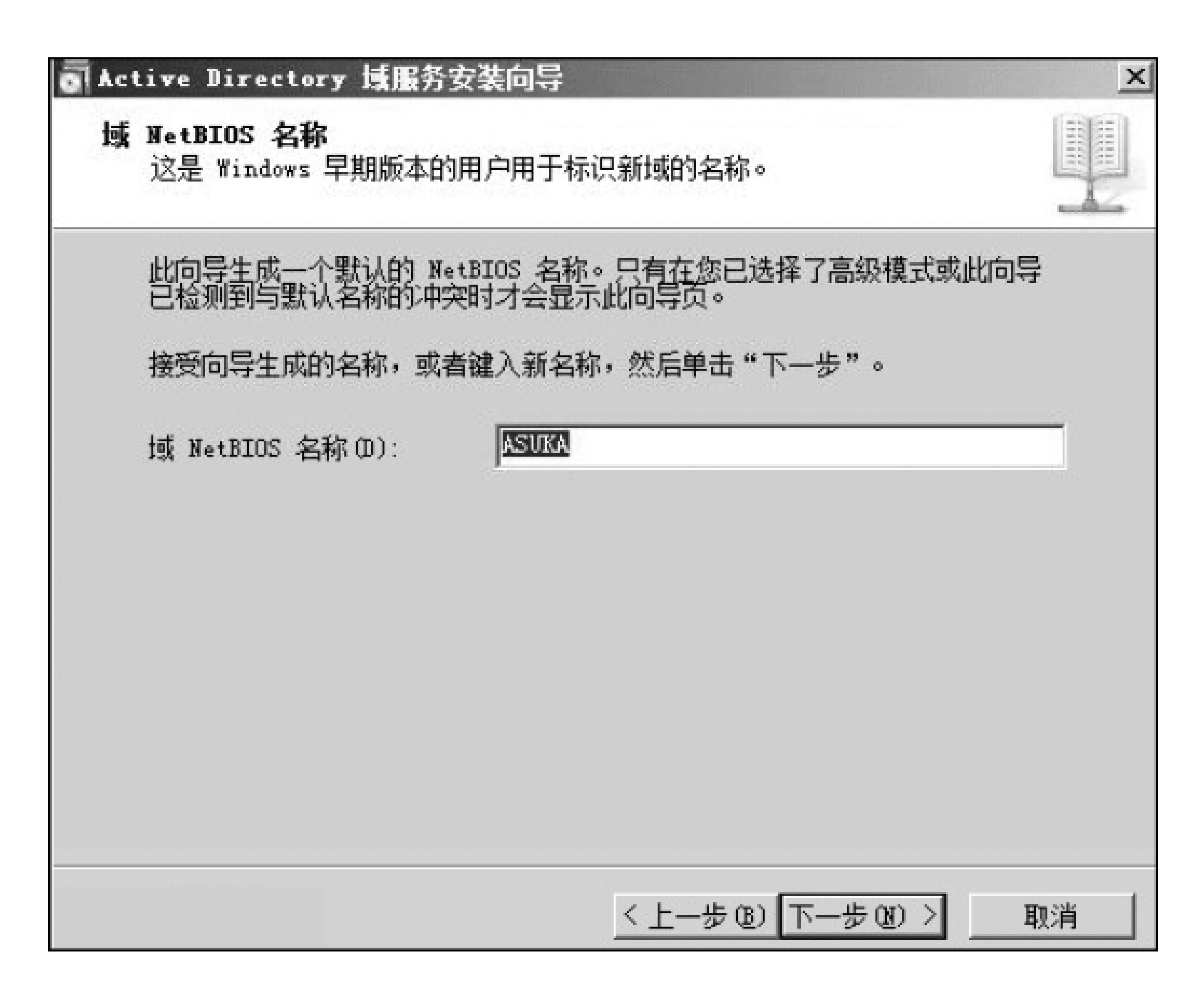


图 2-41　域 NetBIOS 名称

（7）单击"下一步"后出现的对话框如图 2-42 所示。

（8）单击"下一步"后面出现的对话框如图 2-43 所示，选择与服务器所在的站点。

（9）单击"下一步"后出现的对话框如图 2-44 所示，为此控制器选择其他选项。



图 2-42　设置域功能级别



图 2-43　选择一个站点



图 2-44　其他域控制器选项

（10）单击"下一步"后出现的对话框如图2-45所示，选择与控制器相关的数据文件的存储位置。

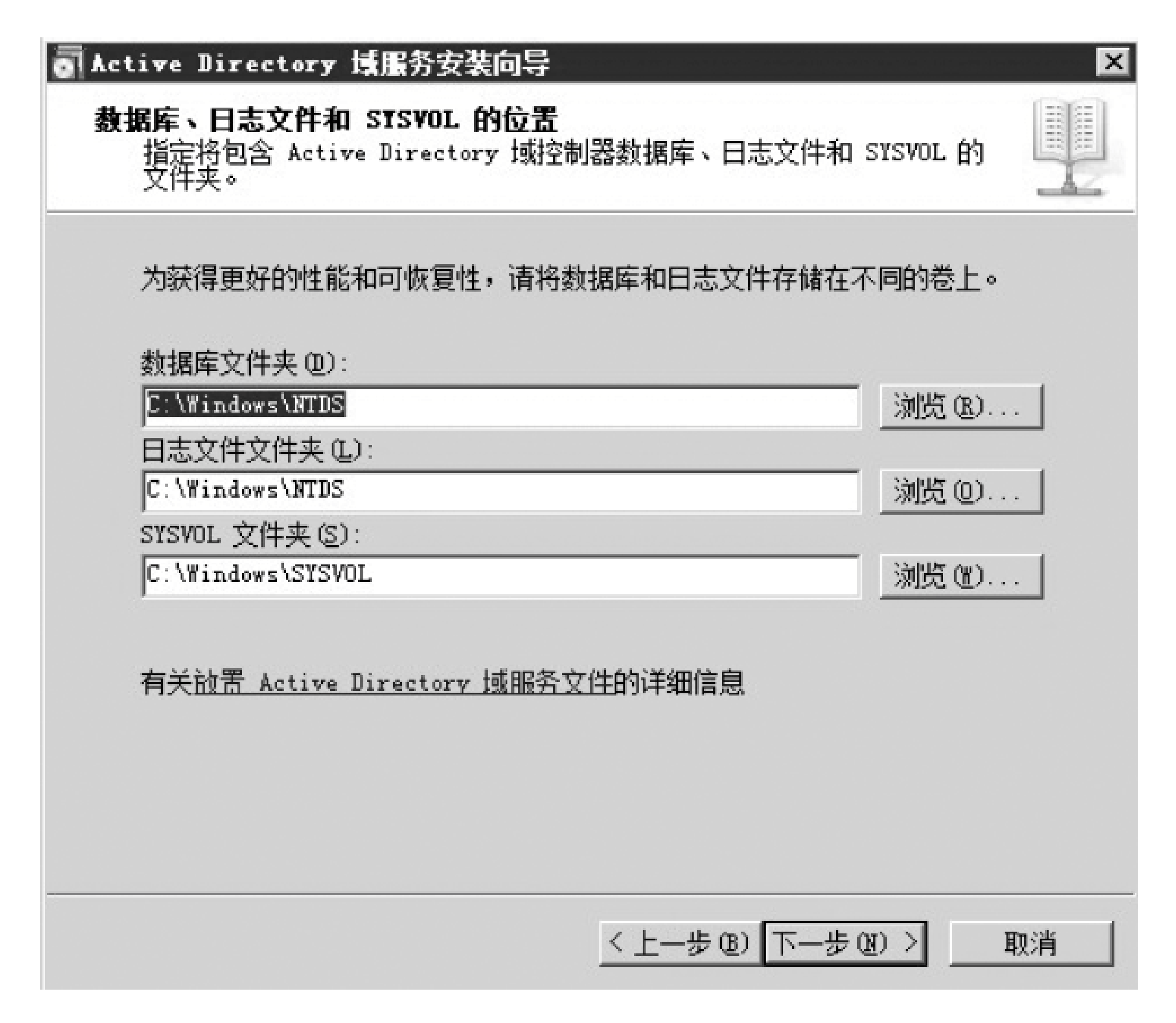


图2-45　数据库、日志文件和SYSVOL的位置

（11）完成子域的建立，如图2-46所示。它为建立子域的"摘要"。

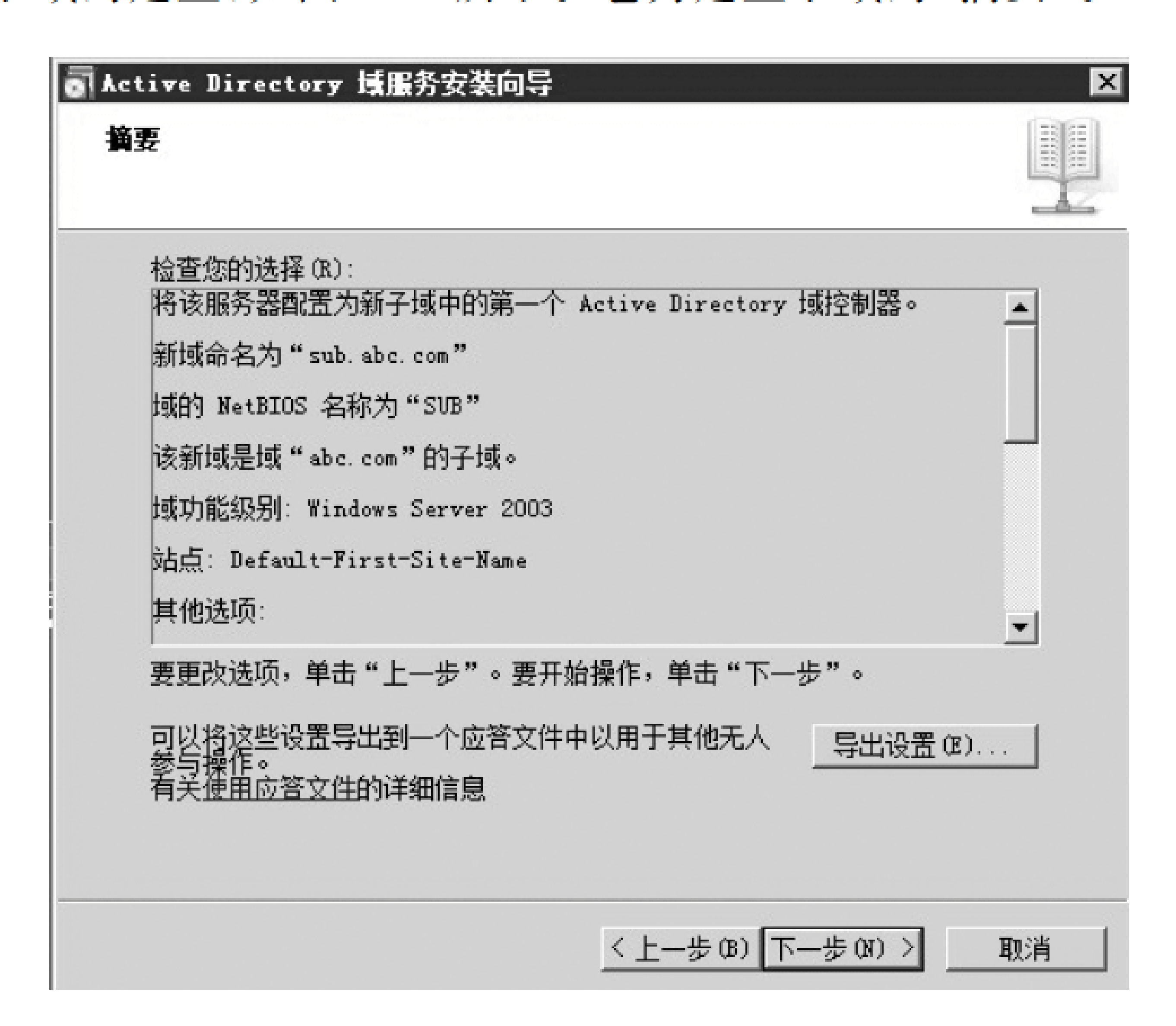


图2-46　子域"摘要"

（12）如果上述摘要显示的不符合要求，我们可以单击"上一步"去进行修改，如果都符合要求则单击"下一步"后完成Active Directory域服务器安装向导，即完成子域sub.abc.com的配置，如图2-47所示。



图 2-47　完成 Active Directory 域服务器安装向导

2.3　创建域环境下的用户、组和 OU

2.3.1　域模式下用户账户的管理

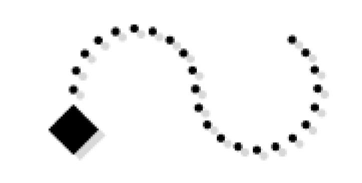
1. 域模式下的账户建立

在已经安装完活动目录，成为域控制器的服务器中的用户的建立是通过“Active Directory 用户和计算机”完成的，具体操作步骤如下：

（1）打开“开始”菜单，选择“管理工具”→“Active Directory 用户和计算机”，如图 2-48 所示。



图 2-48　启动“Active Dircetory 用户和计算机”



（2）启动“Active Dircetory 用户和计算机”后，在控制台中右击 Users，依次选择“新建”→“用户”命令，如图 2-49 所示。

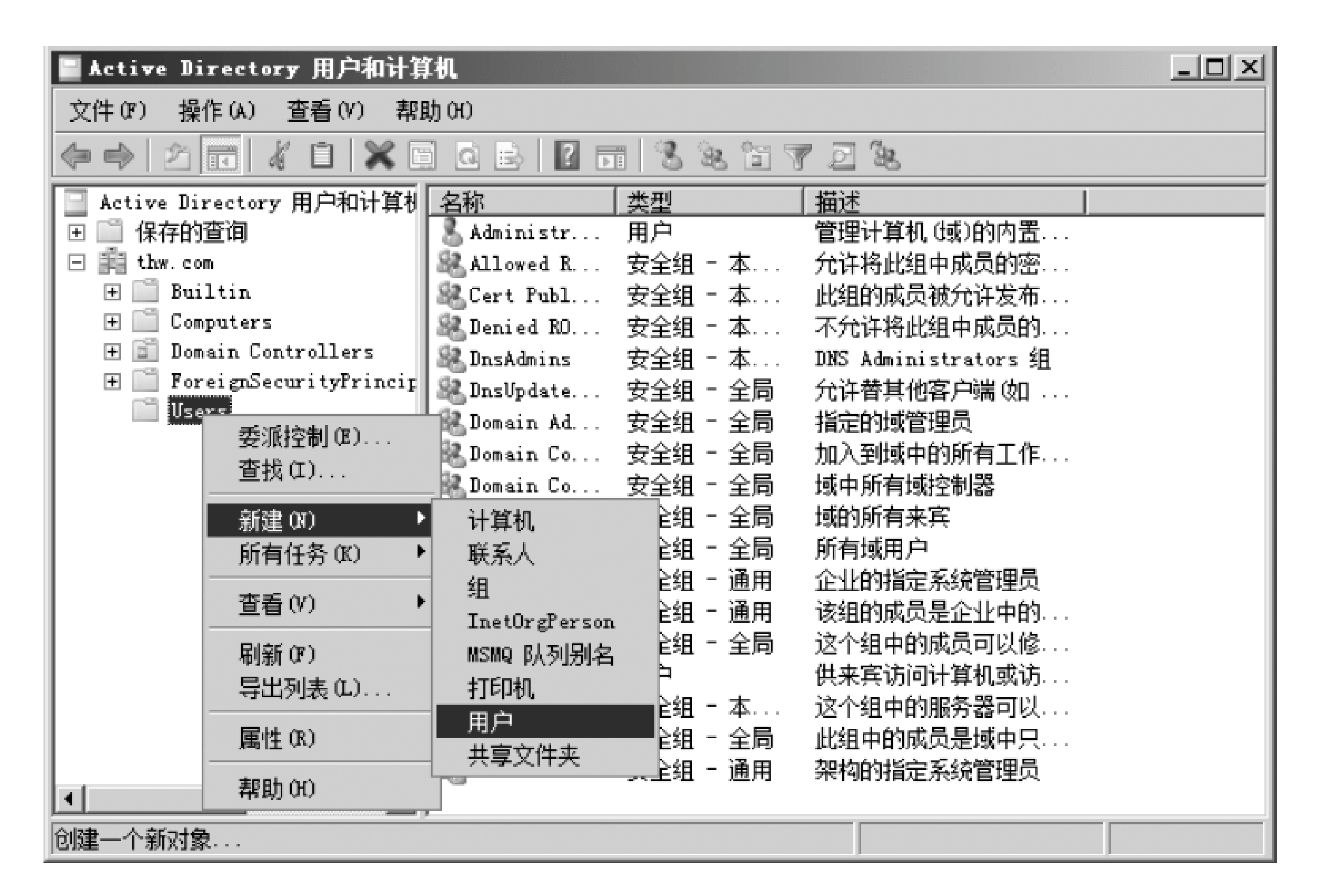


图 2-49　创建用户

（3）在“新建对象-用户”对话框中输入用户的姓名及用户登录信息，如图 2-50 所示。

新建对象 - 用户

创建于：　thw.com/Users

姓(L)：t1

名(F)：　　英文缩写(I)：

姓名(A)：t1

用户登录名(U)：

t1　@thw.com

用户登录名(Windows 2000 以前版本)(W)：

THW\　t1

< 上一步(B)　下一步(N) >　取消

图 2-50　输入账户信息(1)

注意：在输入账户信息时，可以输入中文作为用户登录名。“新建对象”中登录名是该账户登录域时使用的名字，姓、名的输入内容只是作为账户登录信息，与登录域时输入的账号无关。

（4）单击“下一步”按钮为用户设置密码，其操作与第 1 章建立账户的操作相同，按照中文向导操作提示完成，如图 2-51 所示。

在建立密码后对话框中有 4 个选项，分别表示密码使用时的设置方式。

- 用户下次登录时需更改密码，表示该账户第一次登录域中的计算机时，系统要求

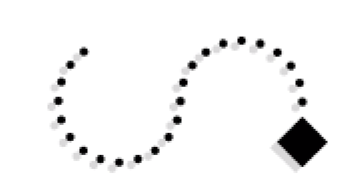




图 2-51　输入账户信息(2)

你必须更改密码，这样保证用户自己掌握自身账户的密码。

- 用户不能更改密码，表示账户自己没有权利对自身账户密码进行修改，必须通过域控制器管理员完成。
- 密码永不过期，表示账户设置的密码，不会因系统默认密码有效期到期而要求用户修改，密码始终有效。
- 账户已停用，表示当前账户如果不能在域中继续使用，则选择该项，使账户停用，而不是删除账户信息。

2. 域模式下的账户属性

域账户是在域范围内都可以登录的用户，这就需要用户向系统提供更多信息，以便于向域中有权索取账户信息部门提供有效的信息。域模式下的账户管理涵盖了用户如下信息，如图 2-52 所示。

在图 2-52 中，出现了十多项选项，涵盖了账户的很多信息，下面简单介绍一下。

常规、地址、电话、单位标签，这些信息是账户的个人信息，用于拥有权限的账户查询。

账户选项卡的上半部分与本地账户信息没有区别，但下半部分包括了众多的信息，它们主要是有关账户安全方面的设置，如图 2-53 所示。其中账户过期是指账户的存活期，可以选择“永不过期”或“在此之后”过期。“在此之后”是指在此日期之后，该用户不能登录到系统中了。

在域控制器管理的网络系统中，账户可以被限制进入系统和使用系统，这种限制归纳为 5 个指定，即

- 指定的账户——用户进入计算机的凭证。
- 指定的计算机——用户在指定的计算机进入系统。
- 指定的时间——用户在规定的时间进入系统。
- 运行指定的程序——用户只能调用指定的应用软件。
- 访问指定资源——用户只能访问指定的文件夹和对文件夹进行指定的处理。

图 2-52　账户常规信息

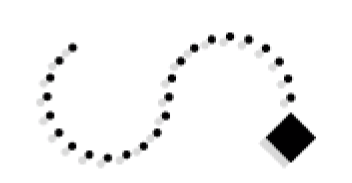
图 2-53　账户选项

在这 5 个指定中，“指定的计算机”和“指定的时间”是在账户设置中完成的。“指定的计算机”就是“登录到”按钮对应的选项，如图 2-54 所示。



图 2-54　账户在指定计算机登录

用户可以在所有计算机登录，也可被限制在指定的计算机上登录，在图 2-54 中单击“所有计算机”单选按钮，就是允许该账户可以通过任何计算机登录。但是在企业实际应用中，出于对特殊用户的安全要求，是不允许使用非本人使用的专用计算机或部门之外的



计算机的，这时，这些用户的登录地点就要进行约束，例如：财务部门的用户，不能随意使用网络中的任何计算机而只能在财务办公室使用本部门计算机，因此这样的用户就需要在此进行设置。

当单击"下列计算机"单选按钮时，就会出现输入计算机名提示，这时请输入该账户要登录的计算机名称，然后单击"添加"，这样该账户就只能通过指定计算机登录到域控制器管理的网络系统中了。如果该用户需要从多台计算机登录，可重复输入多台计算机的名称，如图 2-55 所示。

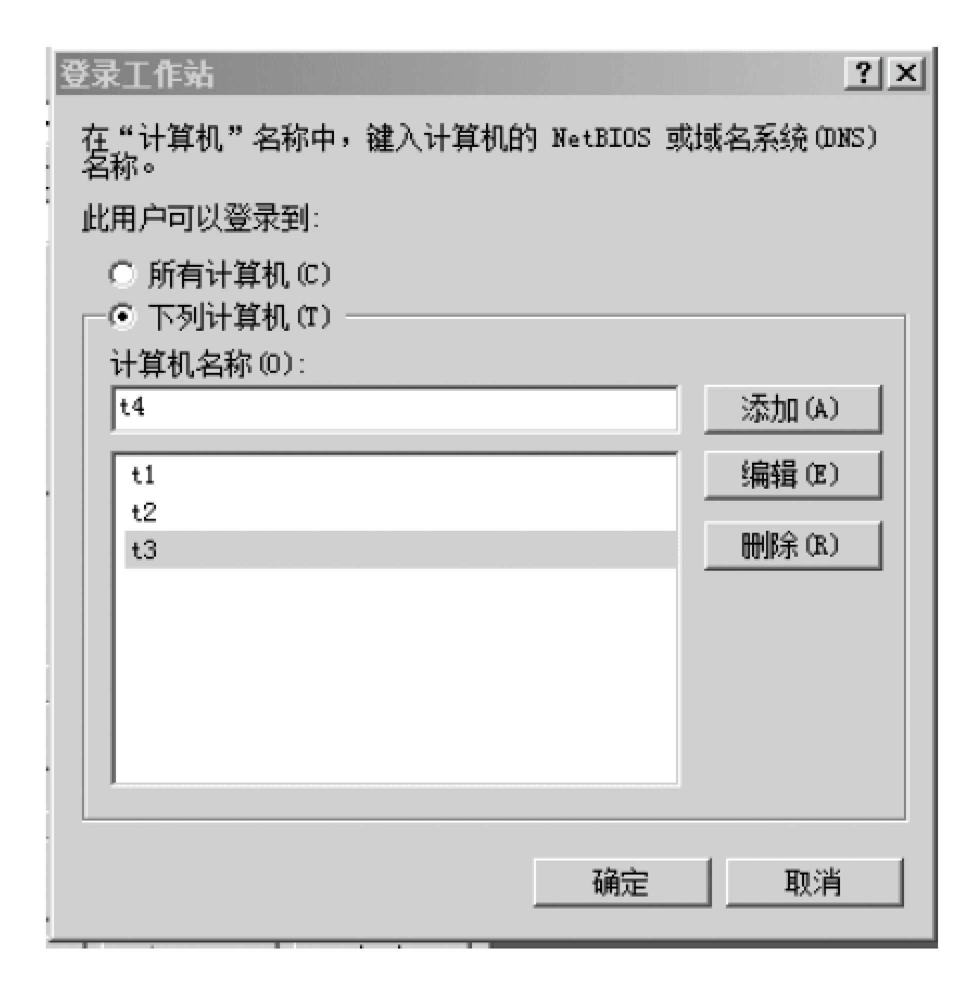


图 2-55　账户从多台指定计算机登录设置

在"指定的时间"设置中，对登录域控制器的账户可以限制在一个特定的时间范围内，单击"登录时间"出现如图 2-56 所示的提示。在登录时间设置对话框中可以设置指定的日期和指定的时间，使得用户只能在规定的时间内登录域控制器。

运行指定程序和访问制定资源通过其他技术手段实现，我们在后面会讲到。

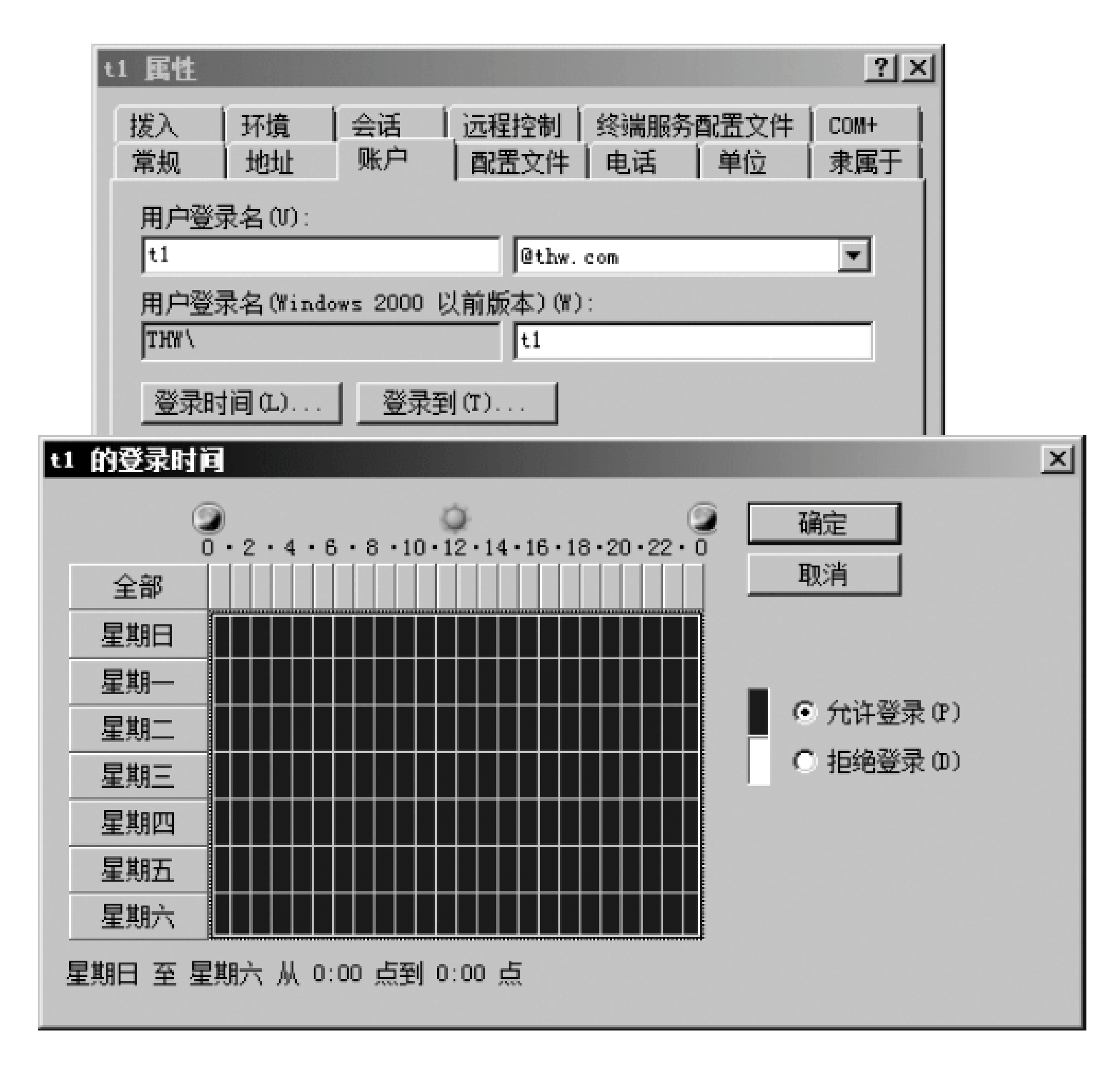


图 2-56　账户登录时间设置

3. 账户的删除

在我们日常的系统管理中，主要是对系统资源和账户的管理，在账户管理中经常出现原来创建的账户不使用的情况，主要有：实验用账户，误操作建立的账户，临时账户和禁用的账户，对于这些账户，只有在一个账户真正作废不用才有删除的必要，建议对暂时不使用的账户先禁用。过了一段时间后，再删除被禁用的账户。

2.3.2 域模式下组的管理

通过设置用户组的属性，可以设置用户组的作用域，组类型、其所包含的用户、所隶属的用户组及管理者等内容。在实际组的使用时，有关组的设置包括以下几个具体的工作，通过以下工作对组进行有效的维护。

1. 组账号建立

域模式下组的建立具体操作如下：

打开“Active Directory 用户和计算机”工具中的 Users 文件夹，依次选择“新建”→“组”命令，如图 2-57 所示。

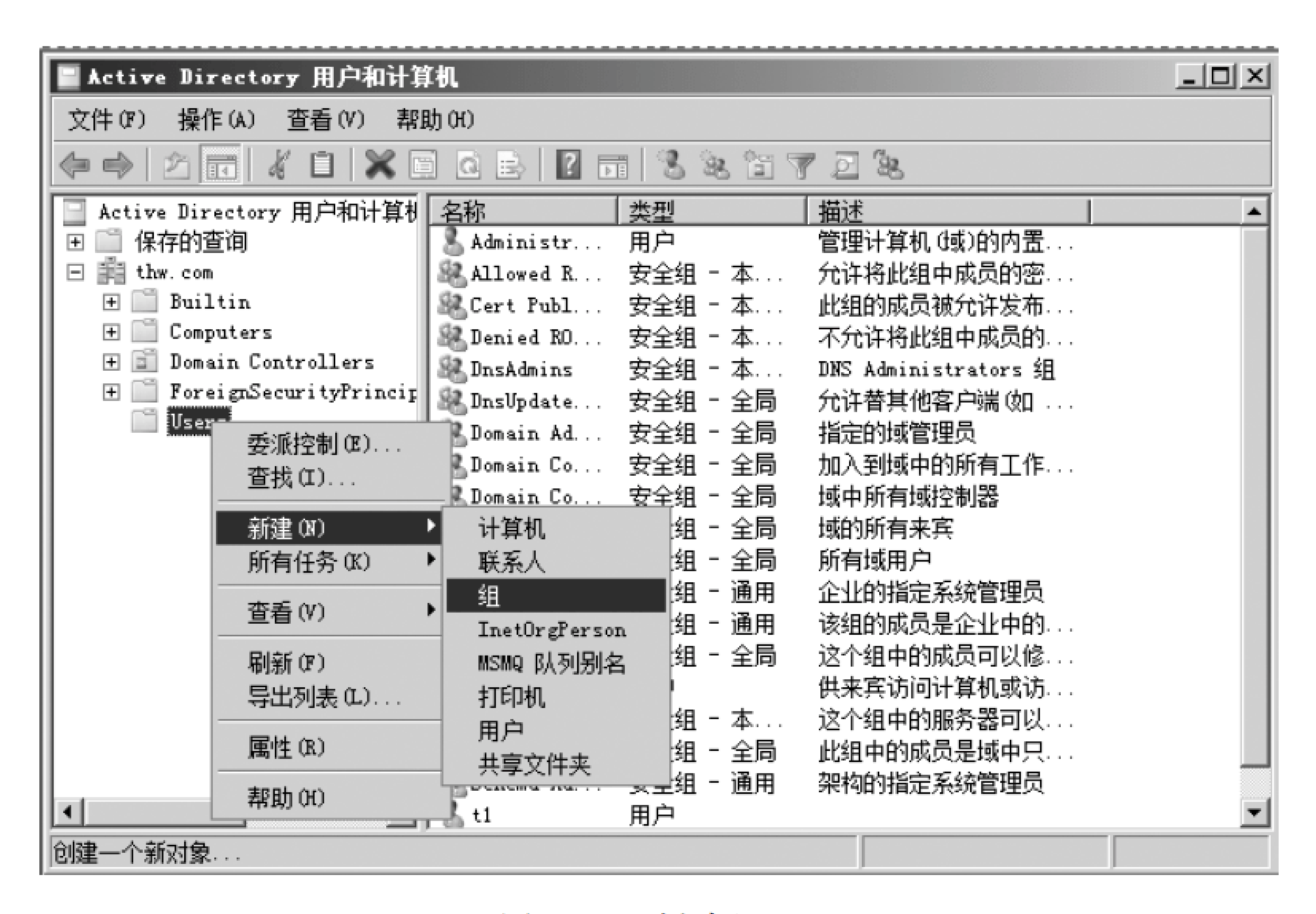


图 2-57　创建组(1)

在创建组对话框中输入属性相应的信息并设置组作用域、组类型，然后单击“确定”，如图 2-58 所示。



图 2-58　创建组(2)

2. 组成员的添加

(1) 打开选择要加入账户的指定组的属性窗口,并单击"成员"标签,如图 2-59 所示。

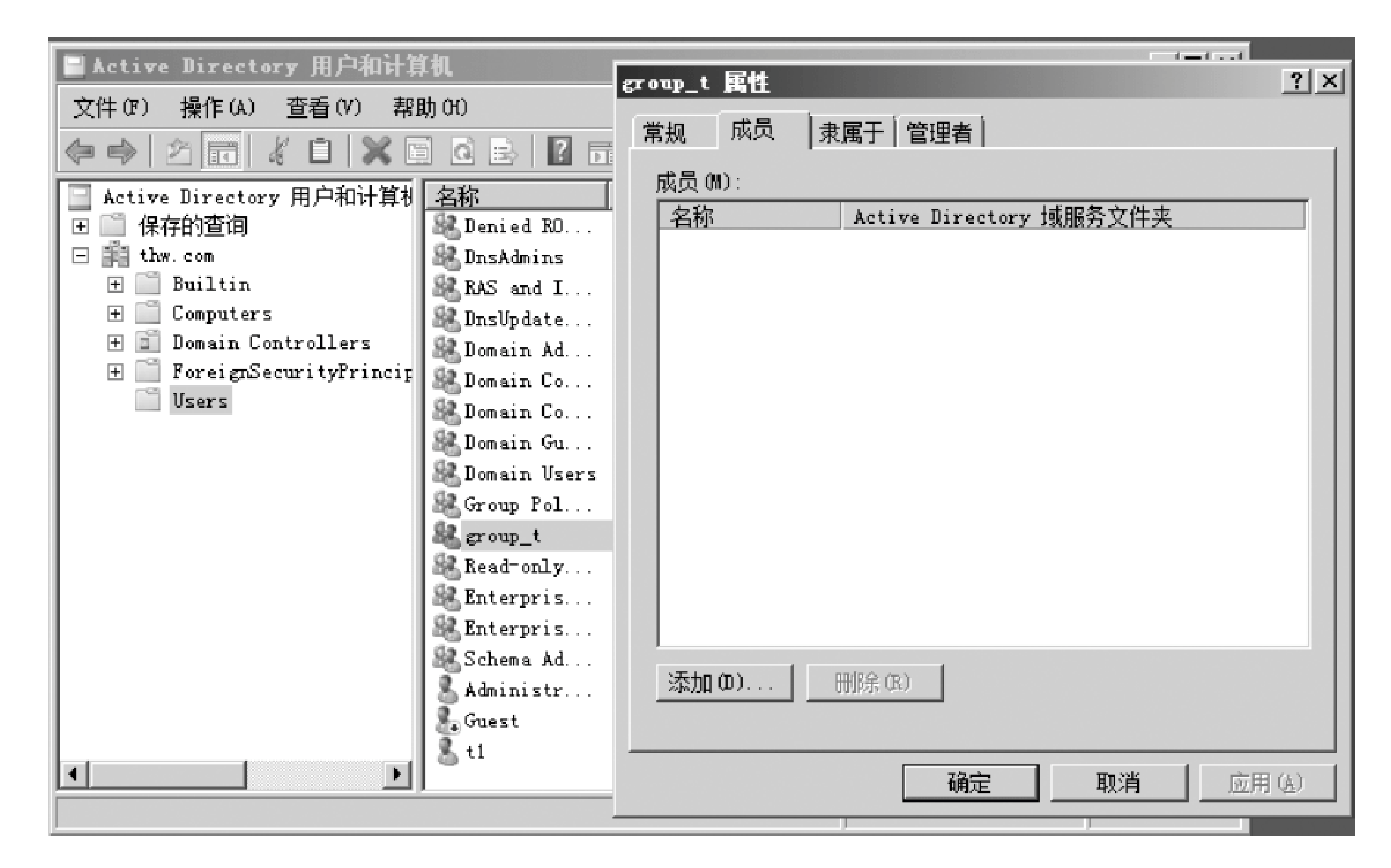


图 2-59　组属性中的成员选项卡

(2) 单击"添加"→"高级"→"立即查找"命令,出现被选用户账户,如图 2-60 所示。

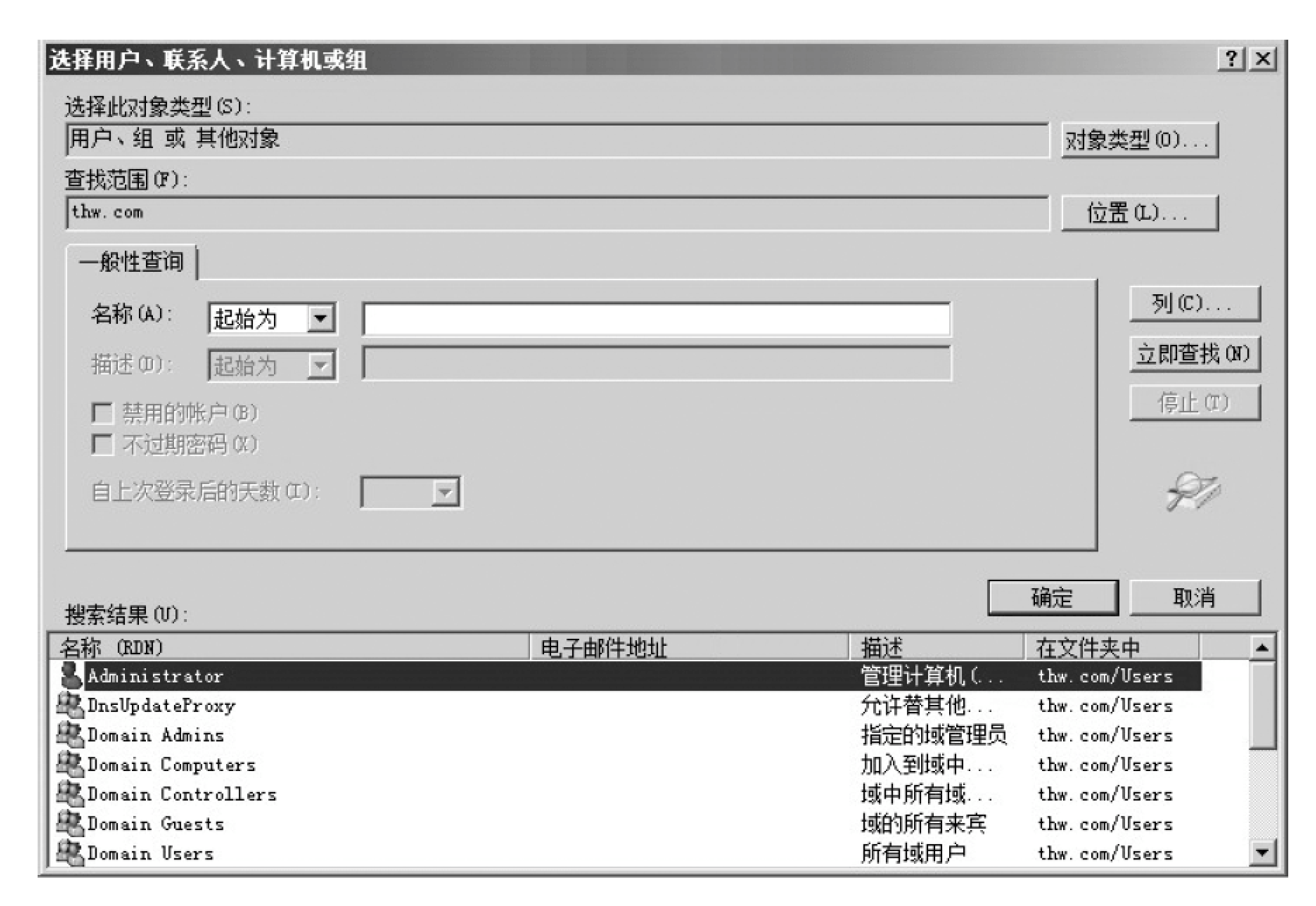


图 2-60　查找账户

(3) 选中要加入组的用户账户,单击"确定",如图 2-61 和图 2-62 所示,就完成了用户的添加。



图 2-61　添加账户



图 2-62　确定账户(1)

3. 组成员的删除

在指定组对话框选中指定用户，然后单击“删除”按钮，这样就可将指定用户从指定组中删除，如图 2-63 所示。

4. 用户加入组

(1) 打开要加入组账户的指定账户的属性对话框，并单击“隶属于”标签，显示已经配置的组嵌套，在 Windows Server 2008 中，可以在域功能级别的基础上进行组嵌套。在该选项卡中，可以根据需要添加或删除所隶属的组，如图 2-64 所示。



图 2-63　确定账户(2)

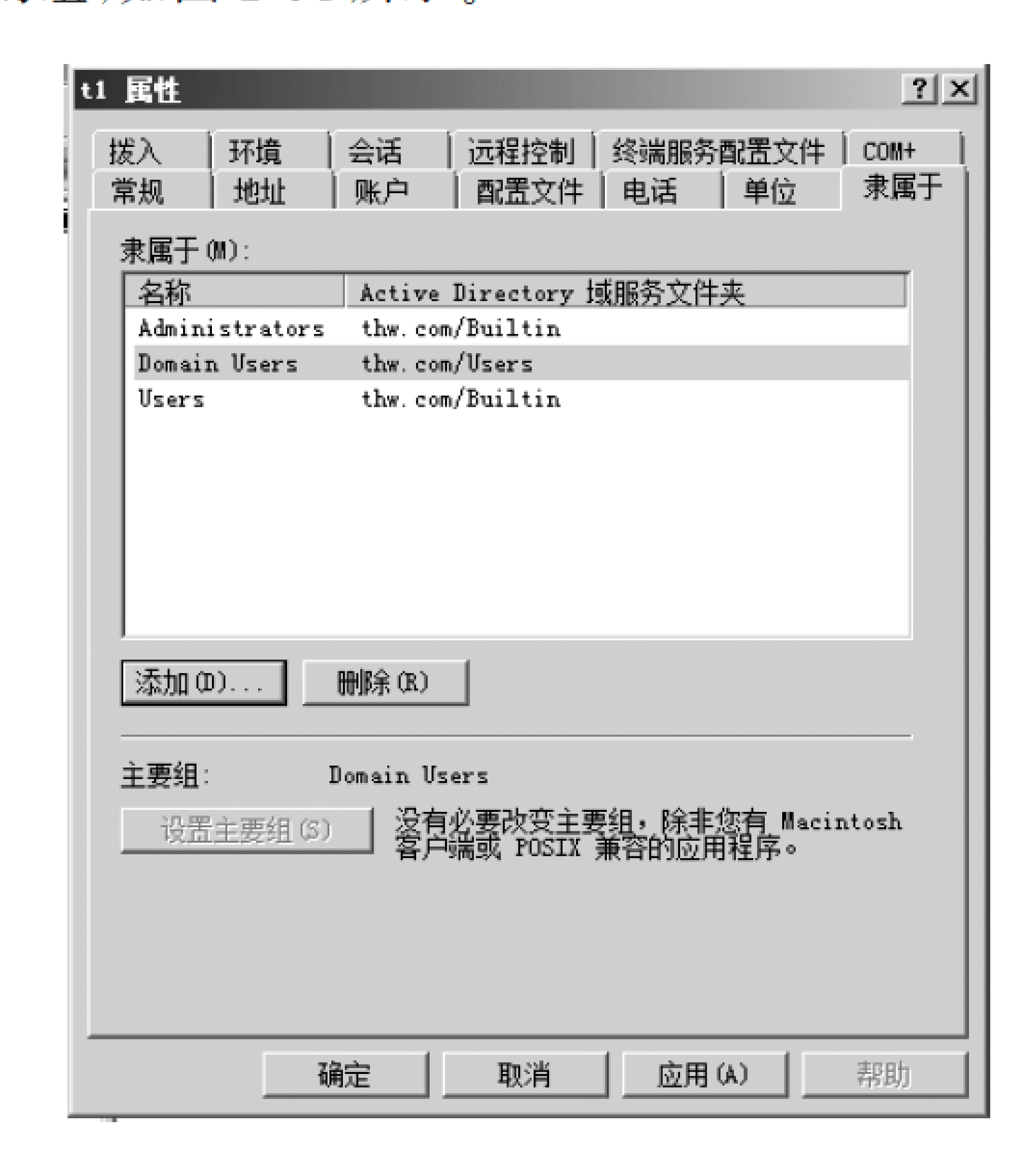


图 2-64　账户属性

(2) 单击“添加”→“高级”→“立即查找”，出现被选组，如图 2-65 所示。



图 2-65　组账户查找

选定要加入的组，单击确定，完成用户账户加入组的操作。

5. 组的重命名

在建立好组账号后，往往因为各种原因要修改组名，这时，组中的成员不变，系统对组权限的设置与管理不会发生任何变化，如图 2-66 所示。



图 2-66　组名修改

6. 组的删除

当一个组需要删除时，可通过在“Active Directory 用户和计算机”工具中选中要删除的组，再选择“删除”选项实现，如图 2-67 所示。



图 2-67 组的删除

2.3.3 域模式下 OU 的建立

本小节我们讲解如何设置 OU。按照以下方法可以建立任何组织单元。

例如要在 thw.com 域建立组织单元 jiaoshi。

(1) 在安装了活动目录的域控制器计算机上单击“开始”→“程序”→“管理工具”命令，打开的界面如图 2-68 所示。

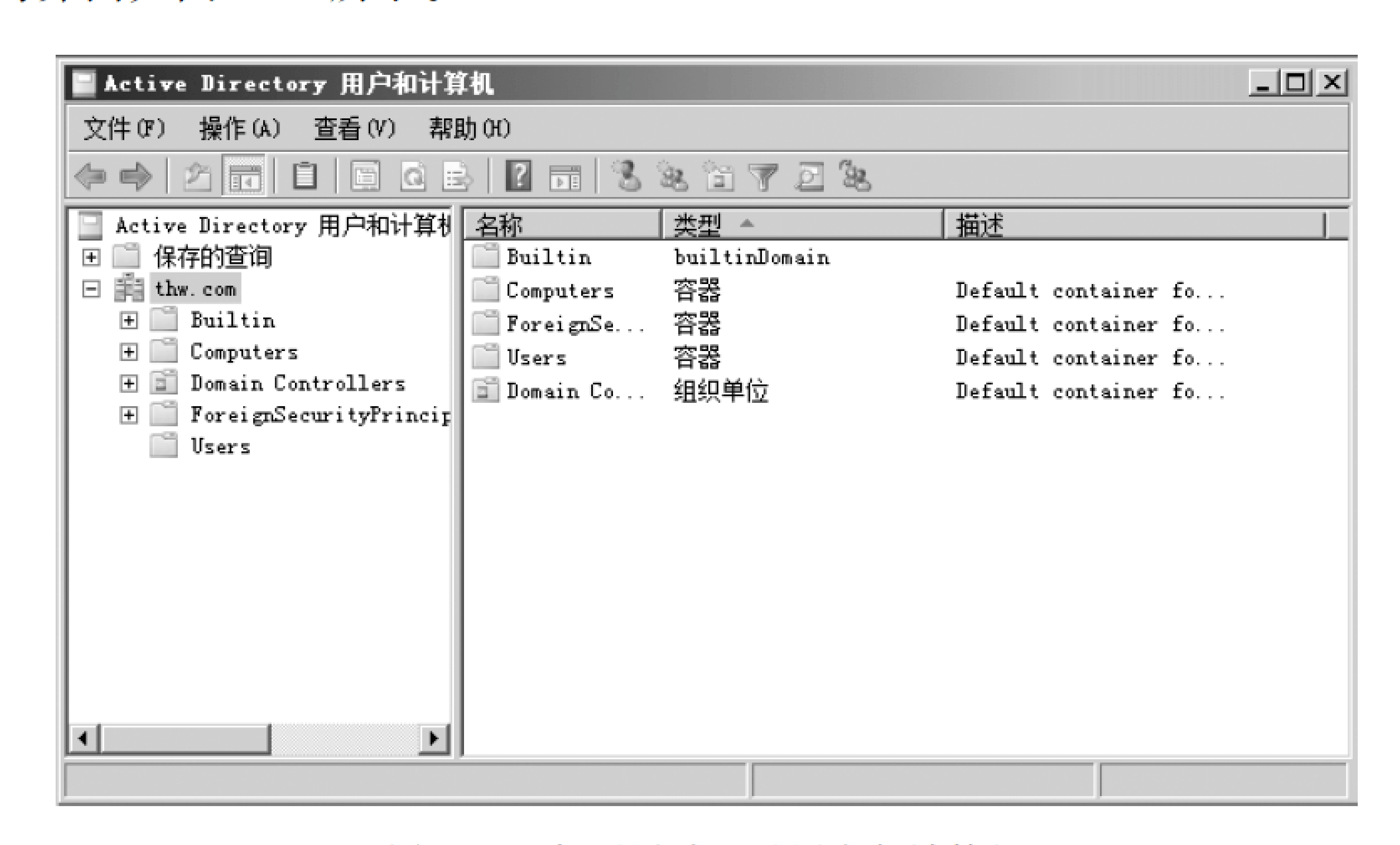


图 2-68 打开活动目录用户与计算机

（2）在 thw. com 空白区域右击，选择“新建”→“组织单元”，如图 2-69 所示。



图 2-69　使用新建命令

（3）单击“组织单元”命令，出现如图 2-70 所示的界面，并在名称栏输入 jiaoshi，单击“确定”完成建立组织单元操作。



图 2-70　创建组织单元 jiaoshi

2.4　客户机加入域

本节讲解如何将计算机加入域，按照下述方法我们可以将任何计算机加入域。例如我们要将 b 计算机加入域（前提条件是网络的数据通信没有问题），需完成以下操作：

（1）调整 TCP/IP 协议的属性，使 DNS 指向域服务器的 DNS，如图 2-71 所示。

（2）在我的电脑上右击，单击“计算机”名标签，如图 2-72 所示。

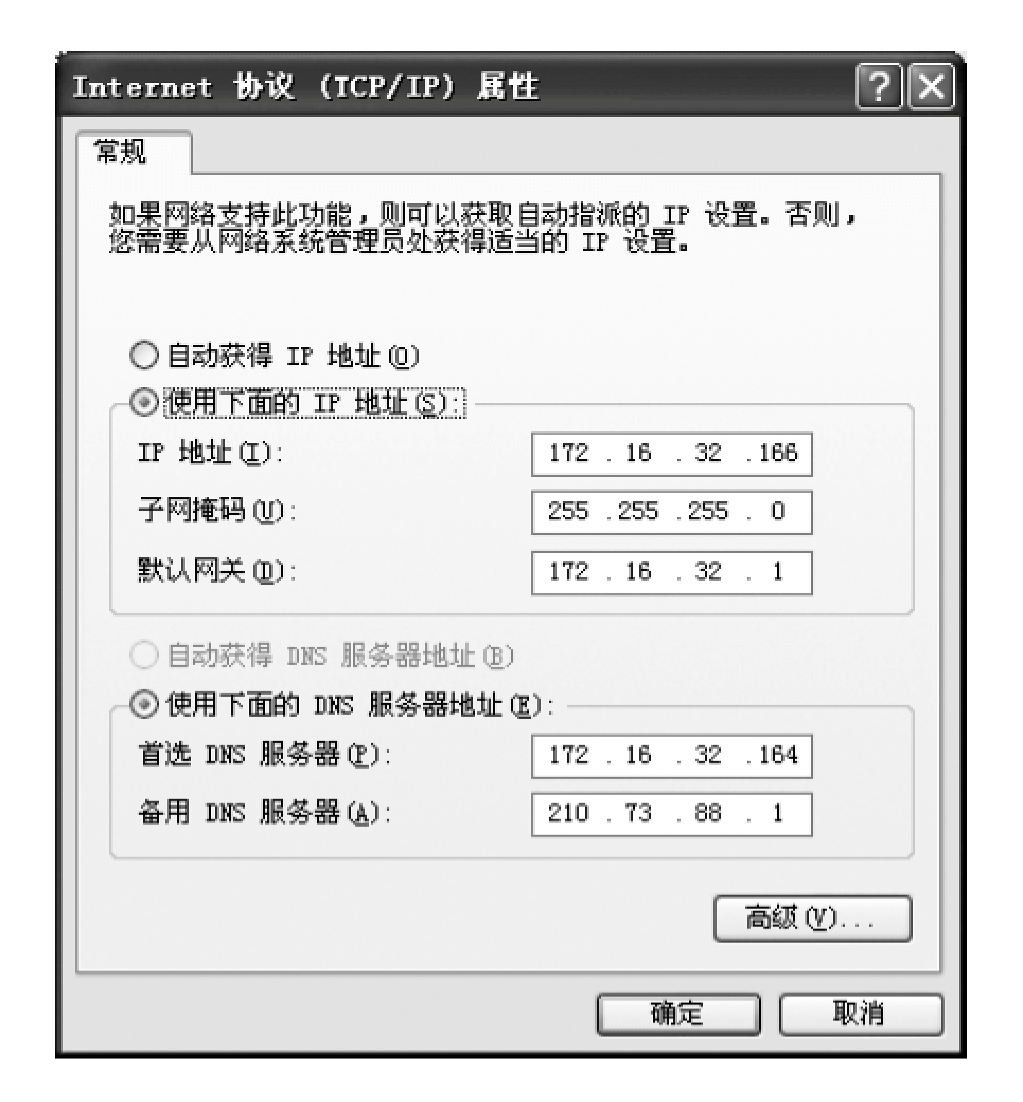


图 2-71　DNS 的调整

图 2-72　计算机名

（3）单击“更改”命令按钮，输入计算机名及加入的域名，如图 2-73 所示。

（4）单击“确定”，出现图 2-74 的界面，输入有操作权的用户名及密码。

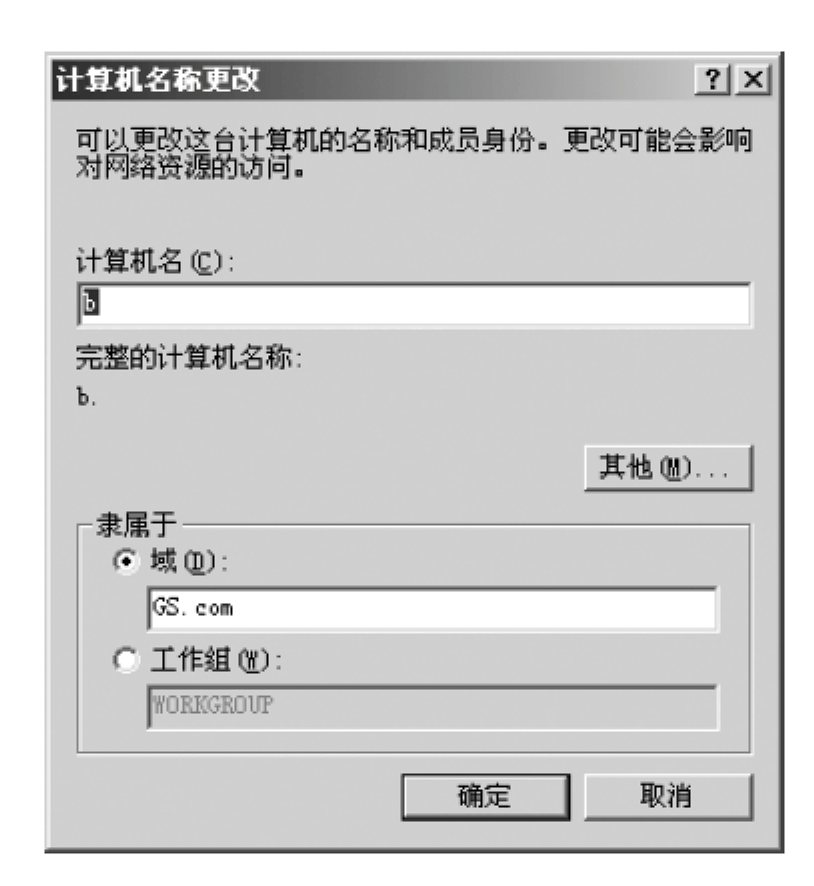


图 2-73　更改操作



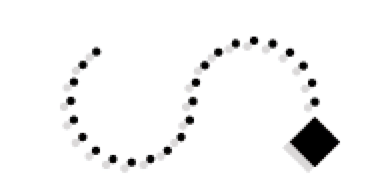
图 2-74　输入用户名及密码

（5）单击“确定”，出现图 2-75 的界面。重新启动计算机，将计算机加入域的工作完成。

将计算机加入域以后，我们就可以在域服务器上对加入域的计算机进行有效的管理了。或在客户机上，通过网上邻居的活动目录项目对其他计算机或域服务器进行有效的管理。如 h1 是 GS.com 的管理员，现在他就可以对域内的计算机包括域服务器进行管理。而这种管理是以管理员的身份登录以后，在域内的任何一台计算机上进行的，不是亲自遍历每一台计算机，充分体现了域工作模式下集中管理的优点。



图 2-75　加入域



本章小结

本章主要讲述了基于活动目录网络的管理思想。要求熟练掌握域、组织单位、群和账户的概念，并在实践中熟练运用这些概念对实际问题建立基于活动目的逻辑空间。熟练掌握在 Windows Server 2008 环境下实现建立域、域树、组织单位、组、账户的操作过程，同时掌握将计算机加入域的操作。进一步理解域模式下网络管理与对等网络模式下网络资源管理的区别。了解服务器在成为域控制器后的变化。

本章习题

1. 简述域、组织单位、组、账户的概念和作用。
2. 简述组与组织单位的区别。
3. 简述网络建立活动目录的意义。
4. 在 Windows Server 2008 下，完成建立域、组织单位、组、账户的实际操作。
5. 将一台计算机加入域。

第 3 章

组策略的应用

【本章重点】

掌握组策略的功能、内容、管理与维护方法。掌握用组策略进行桌面设置、收藏夹和链接、文件夹重定向和硬件访问策略的设置方法与操作要点。掌握通过组策略进行程序的远程安装和禁止运行的技术和操作技巧。

组策略(Group Policy,GP)是系统管理员为计算机用户定义的用来控制应用程序,系统设置和管理模板的一种机制,也是一种用于管理网络内的用户设置和计算机设置的管理工具。所谓组策略,就是基于群体(组织单位、域、站点)的管理策略。它以 Windows 中的一个 MMC 管理单元的形式存在,可以帮助系统管理员针对整个计算机或是微软活动目录的逻辑要素自 Windows NT 4.0 开始便采用了组策略这一机制,经过 Windows 2000 发展到 Windows 2008 已相当完善。

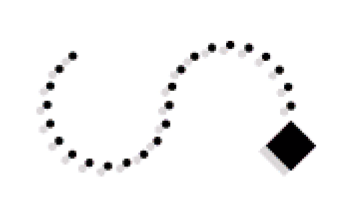
3.1 组策略与组策略对象

组策略是介于控制面板和注册表之间的一种修改系统,是设置程序的工具。一些常用的系统、外观、网络设置等我们可通过控制面板修改,但大家对此肯定都有不满意的地方,因为通过控制面板能修改的东西太少;水平稍高点的用户进而通过修改注册表的方法来设置。我们知道注册表是 Windows 系统中保存系统、应用软件配置的数据库,随着 Windows 功能越来越丰富,注册表里的配置项目也越来越多。

很多配置都是可以自定义设置的,但这些配置分布在注册表的各个角落,如果是手工配置,可想而知是相当困难和繁杂的。而组策略则将系统重要的配置功能汇集成各种配置模块,供管理人员直接使用,从而达到方便管理计算机的目的。组策略使用自己的完善的管理组织方法,对各种对象中的设置进行管理,涉及的内容比控制面板中的多,安全性和控制面板一样非常高,而条理性、可操作性则比注册表强。

3.1.1 组策略的功能

组策略是活动目录的重要组成部分,也是活动目录里的重点内容。使用组策略可以



使工作变得简单化、条理化。利用组策略，用户可以设置多种配置，包括桌面配置和安全配置。例如，可以为特定用户或用户组定制可用的程序、桌面上的内容，以及“开始”菜单选项等，也可以在整个计算机范围内创建特殊的桌面配置。简而言之，组策略是 Windows 中的一套系统更改和配置管理工具的集合。

对于 Windows 9X/NT 用户来说，都知道“系统策略”的概念，其实组策略就是系统策略的高级扩展，它是自 Windows 9X/NT 的“系统策略”发展而来的，具有更多的管理模板、更灵活的设置对象及更多的功能，主要应用于 Windows 2000/XP/2003/7/2008 操作系统中。而系统策略只具有写入注册表项这一个功能，组策略可以完成更多的功能。

早期系统策略的运行机制是通过策略管理模板，定义特定的 POL（通常是 Config.pol）文件。当用户登录时，它会重写注册表中的设置值。当然，系统策略编辑器也支持对当前注册表的修改，另外也支持连接网络计算机并对其注册表进行设置。

而组策略及其工具，则是对当前注册表进行直接修改。显然，Windows 2000/XP/2003 系统的网络功能是其最大的特色，所以其网络功能自然是不可少的，因此组策略工具还可以打开网络上的计算机进行配置，甚至可以打开某个 Active Directory（活动目录）对象（即站点、域或组织单位）并对其进行设置。这是以前“系统策略编辑器”工具无法做到的。

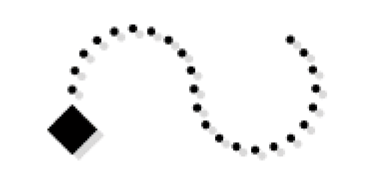
当然，无论是“系统策略”还是“组策略”，它们的基本原理都是修改注册表中相应的配置项目，从而达到配置计算机的目的，只是它们的一些运行机制发生了变化和扩展而已。

3.1.2　组策略的内容

计算机组策略主要可进行两个方面的配置：计算机配置和用户配置。“计算机配置”是对整个计算机中的系统配置进行设置，它对当前计算机中所有用户的运行环境都起作用；“用户配置”则是对当前用户的系统配置进行设置，它仅对当前用户起作用。例如“计算机配置”和“用户配置”都提供了“停用自动播放”功能的设置，但效果是不同的；如果是在“计算机配置”中选择了该功能，那么所有用户的光盘自动运行功能都会失效；如果是在“用户配置”中选择了该功能，那么仅仅是该用户的光盘自动运行功能失效，其他用户则不受影响。

当计算机配置与用户配置发生矛盾时，计算机配置优先。其下所有设置项的配置都将保存到注册表的相关项目中。计算机配置保存到注册表的 HKEY_LOCAL_MACHINE 子树中，用户配置保存到 HKEY_CURRENT_USER。在 Windows 2008 以及 Windows 2003 中，组策略一般放在“系统安装:\windows\system32\GroupPolicy”文件夹中，文件名为 gpedit.msc。

如图 3-1 所示，组策略分为两大部分：计算机配置和用户配置。每一个部分都有自己的独立性，因为它们配置的对象类型不同。计算机账户部分控制计算机账户，同样用户配置部分控制用户账户。其中有部分配置在计算机部分拥有且在用户部分也有同样的配置，它们是不会跨越执行的。假设某个配置选项你希望计算机账户启用、用户账户也启用，那么就必须在计算机配置和用户配置部分都进行设置。总之计算机配置下的设置仅对计算机对象生效，用户配置下的设置仅对用户对象生效。



分别展开“计算机配置”和“用户配置”会发现还有以下三个项目，如图 3-1 所示。



图 3-1　组策略对象界面

- 软件设置：用于对已经安装好的软件进行管理和维护。
- Windows 设置：用于系统或用户的开关机脚本，系统安全等内容的设置。
- 管理模块：主要用于对系统、网络、Windows 组件等内容进行设置，还可以添加或者删除管理模块。

组策略是 Windows 2008 中提供的一种重要的更新和配置管理技术。它与域或组织单位结合，就能控制和管理网络中的域用户和计算机的工作环境。它有几千项配置，主要包括以下功能：用户工作环境的设置，安全设置，软件的安装与删除，脚本的设置，文件夹重定向。

在域环境内可以有成百上千个组策略能够创建和存在于活动目录中，并且能够通过活动目录这个集中控制技术，实现对整个计算机、用户和网络的基于组策略的控制管理。在活动目录中我们可以为站点、域、OU 创建不同管理要求的组策略，而且允许每一个站点、域、OU 能同时设置多套组策略。

3.1.3　创建和链接组策略对象

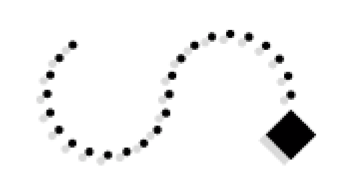
组策略设置存储在组策略对象（GPO）中，即组策略是由具体的组策略对象来实现的。根据组策略对象的作用范围，可分为以下两种。

本地组策略对象：它只存在一台计算机上，只对本地用户及该计算机起作用。

Active Dirctory 组策略对象：存储在控制器上，只能在活动目录环境下使用，适用于组策略所作用的站点、域、组织机构中的用户和计算机。

当多个组策略在一起时，执行的顺序是本地组策略、活动目录的站点策略、活动目录的域策略、活动目录的组织单位策略。这些策略不一致时，后应用的策略覆盖前一个策略。在活动目录层次结构的每一级组织单位中，可以链接一个、多个或不链接组策略对象，如果一个组织对象链接了多个组策略，则按管理员制定的顺序处理，较前位置的组策略具有较高的优先权。

下面我们就说明如何建立组策略和连接组策略。



（1）在 Windows Server 2008 上，以管理员身份登录，依次选择“开始”→“管理工具”→“组策略管理”，如图 3-2 所示。



图 3-2　启动组策略管理

（2）进入组策略管理界面，依次选择“组策略管理”→“林：thw. com”→“域”→thw. com→xuesheng，右击 xueshengOU（组织单元），在弹出的菜单中选择“在这个域中创建 GPO 并在此处链接”选项，如图 3-3 所示。

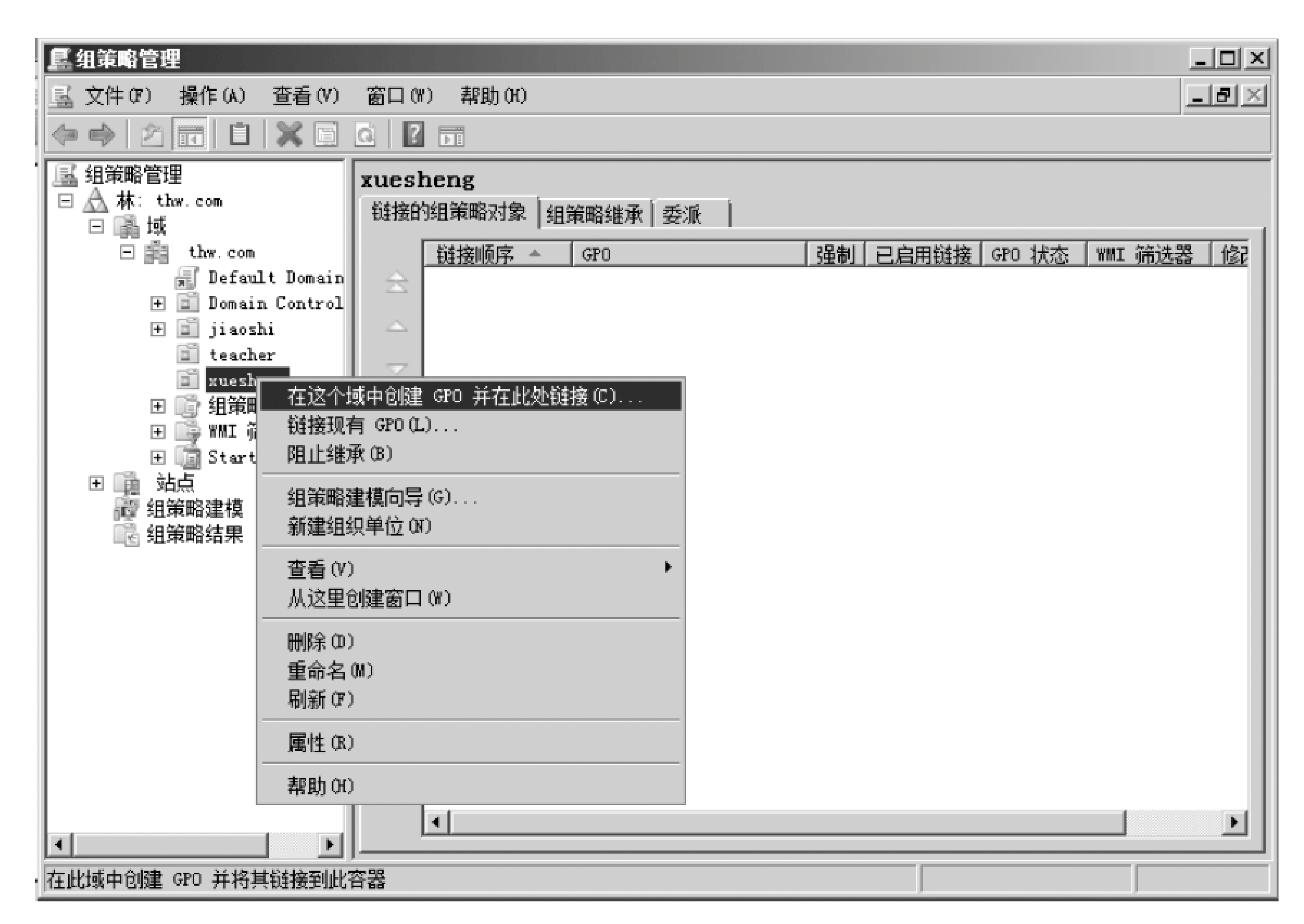
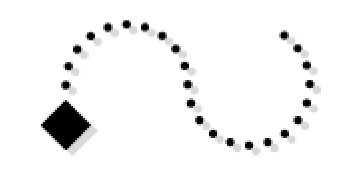


图 3-3　在这个域中创建 GPO 并在此处链接



（3）在弹出的对话框中为新建立的 GPO 起个名字，例如：software OU，如图 3-4 所示。

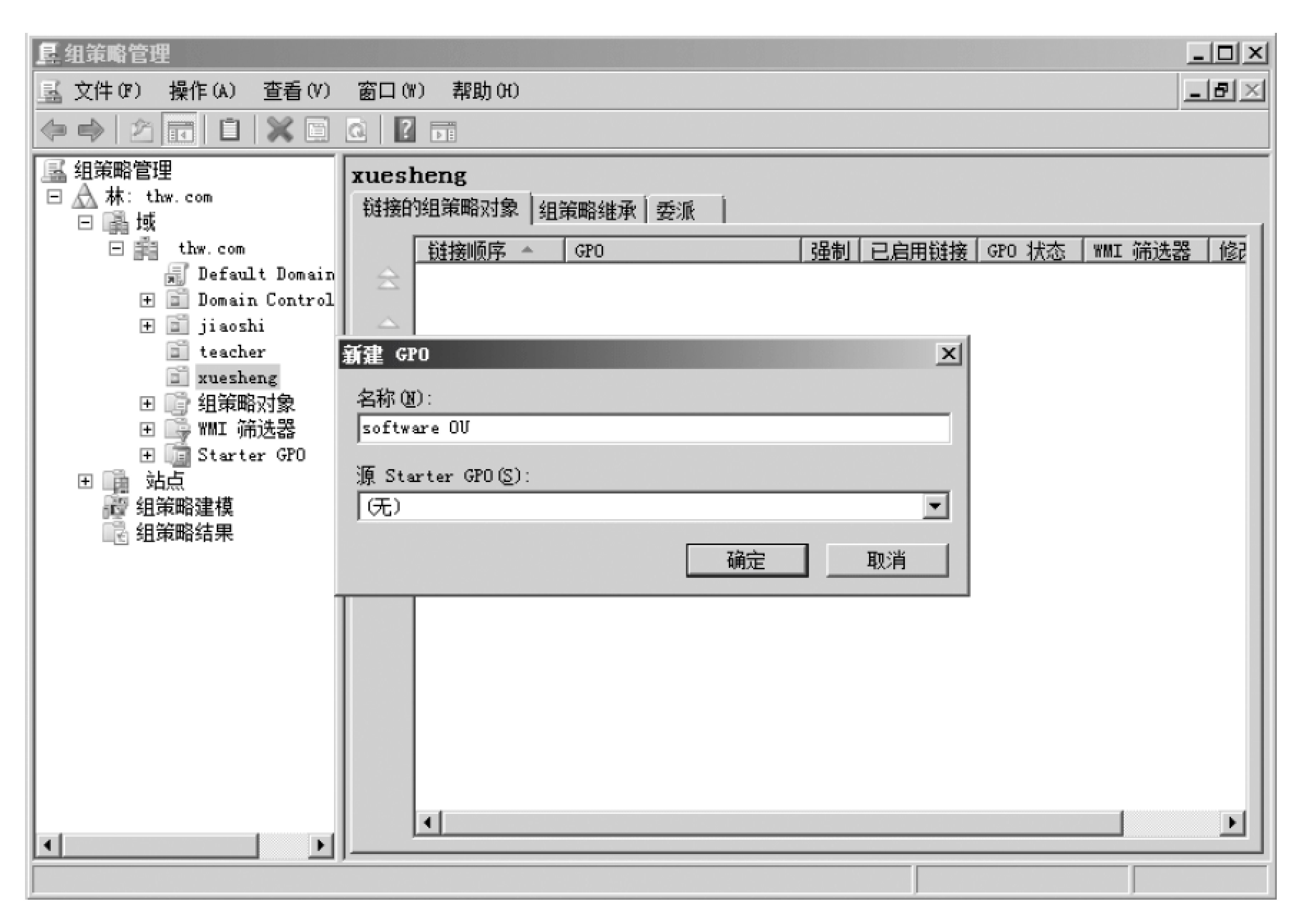


图 3-4　新建组策略

（4）右击新建立的 software OU，在弹出菜单中选择“编辑”，如图 3-5 所示对话框；然后进入组策略管理编辑器，图 3-6 所示。

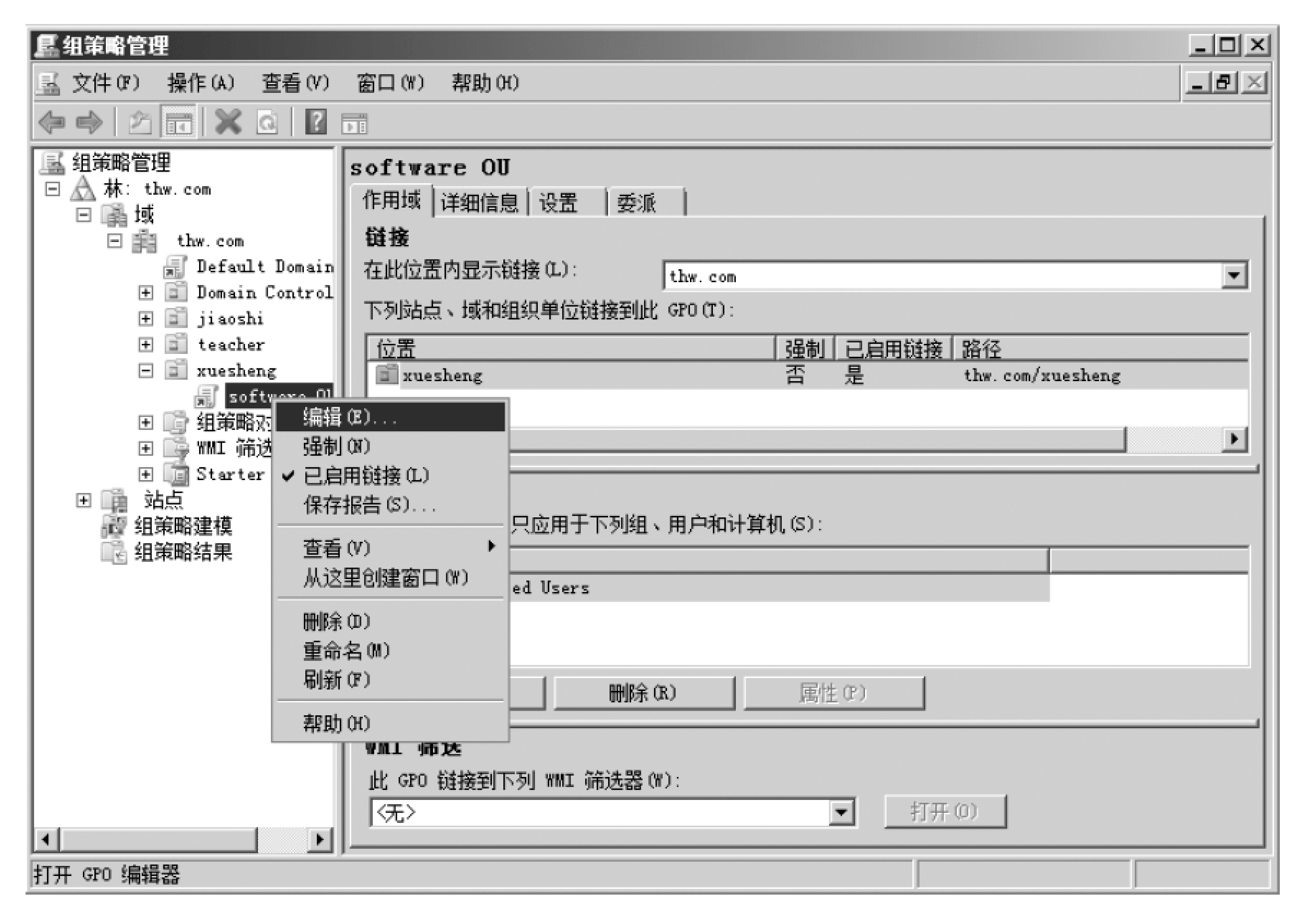


图 3-5　启动组策略管理编辑器

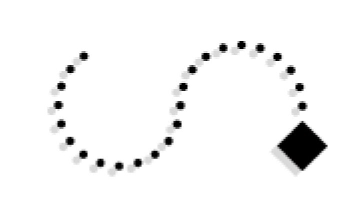




图 3-6　组策略管理编辑器

3.2　通过组策略定制工作环境

3.2.1　修改登录用户的桌面

桌面是打开计算机并登录到 Windows 之后看到的主屏幕区域。就像实际的桌面一样，它是用户工作的平面。打开程序或文件夹时，它们便会出现在桌面上。还可以将一些项目(如文件和文件夹)放在桌面上，并且随意排列它们。有时桌面定义更为广泛，包括任务栏和 Windows 边栏。任务栏位于屏幕的底部，显示正在运行的程序，并可以在它们之间进行切换。它还包含“开始”按钮，使用该按钮可以访问程序、文件夹和计算机设置。边栏位于屏幕的一侧，包含称为小工具的小程序。

下面的操作说明如何设置统一的桌面壁纸。

(1) 打开组策略编辑器，在左侧的目录树中依次选择“用户配置”→“策略”→“管理模板：从本地计算机检索到的策略定义(AIMX 文件)”→“桌面”→“桌面”，在右边的显示视图中会出现可以对桌面进行的配置，如图 3-7 所示。



图 3-7　组策略的桌面配置

（2）选择启动 Active Desktop，如图 3-8 所示。

（3）设置统一桌面墙纸，如图 3-9 所示（已提前将墙纸存入共享文件夹中）。



图 3-8　设置启动 Active Desktop

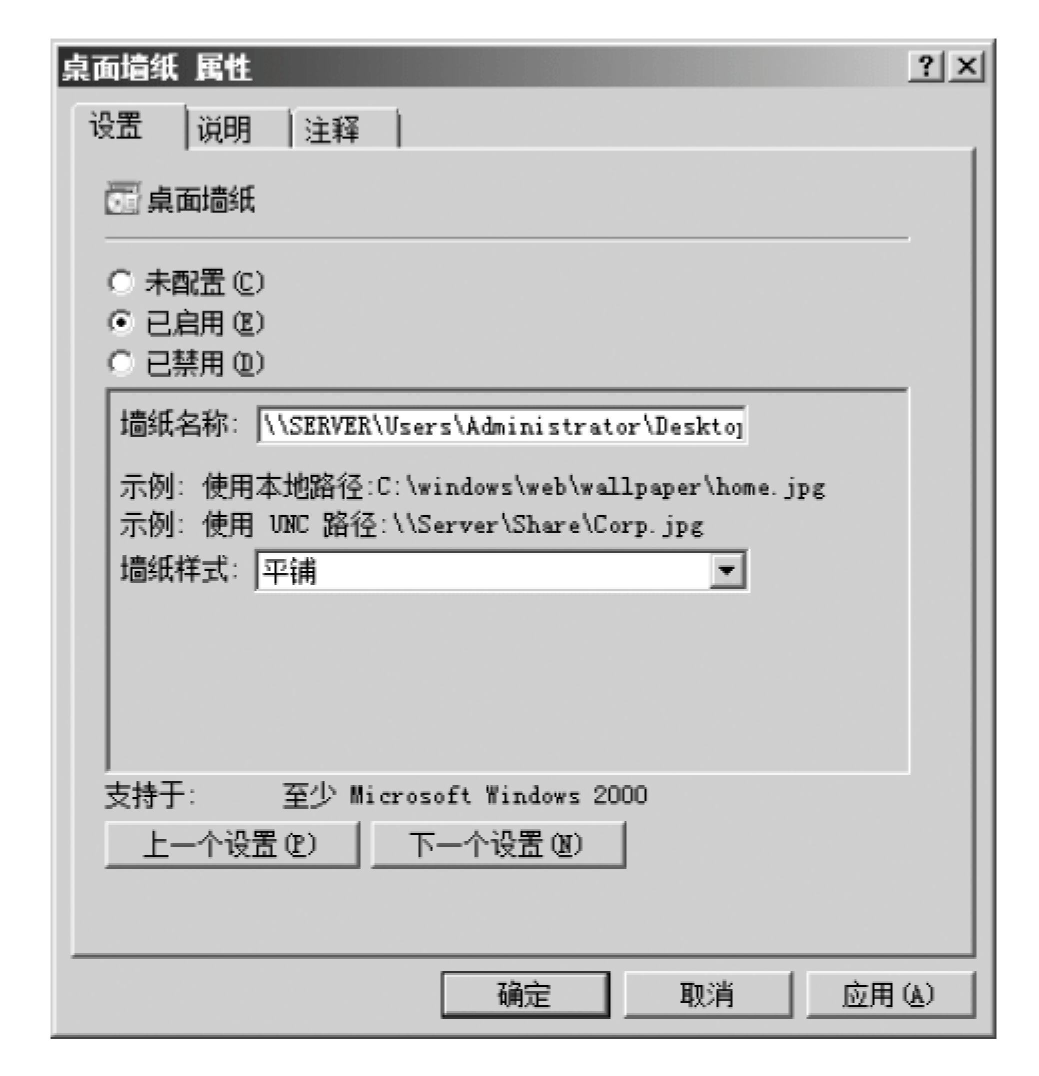


图 3-9　桌面墙纸的设置

（4）设定用户不能自行修改桌面，如图 3-10 所示。

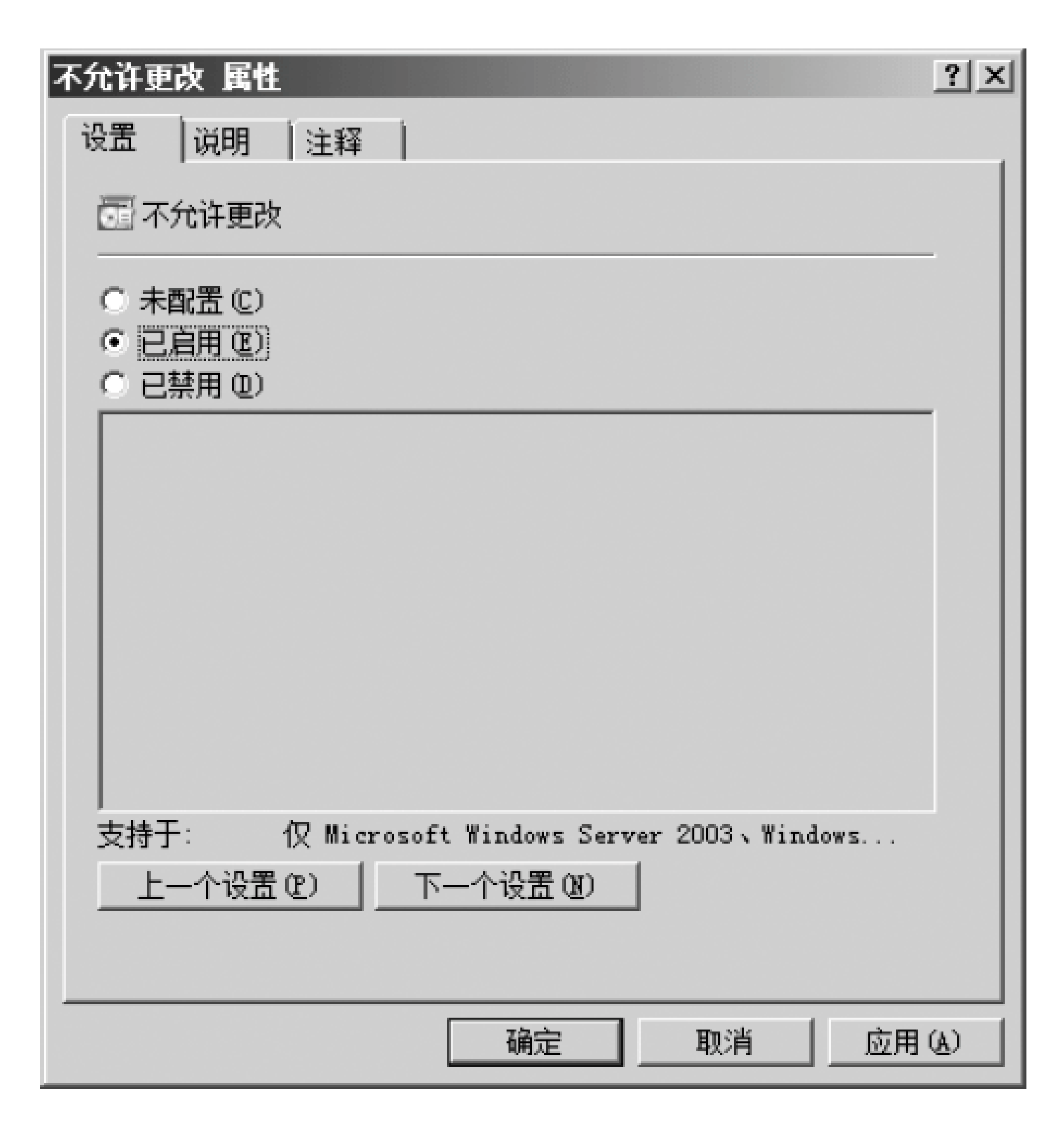
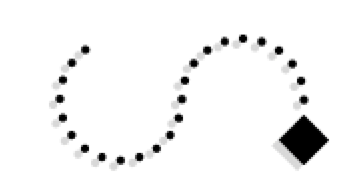


图 3-10　不允许更改设置

（5）以组策略所管辖的用户身份登录客户机，就可看到统一设置的桌面墙纸，如图 3-11 所示。

3.2.2　配置用户的收藏夹和链接

利用组策略可以对用户上网时使用的 IE 浏览器进行有效的管理，如可以禁用导入/



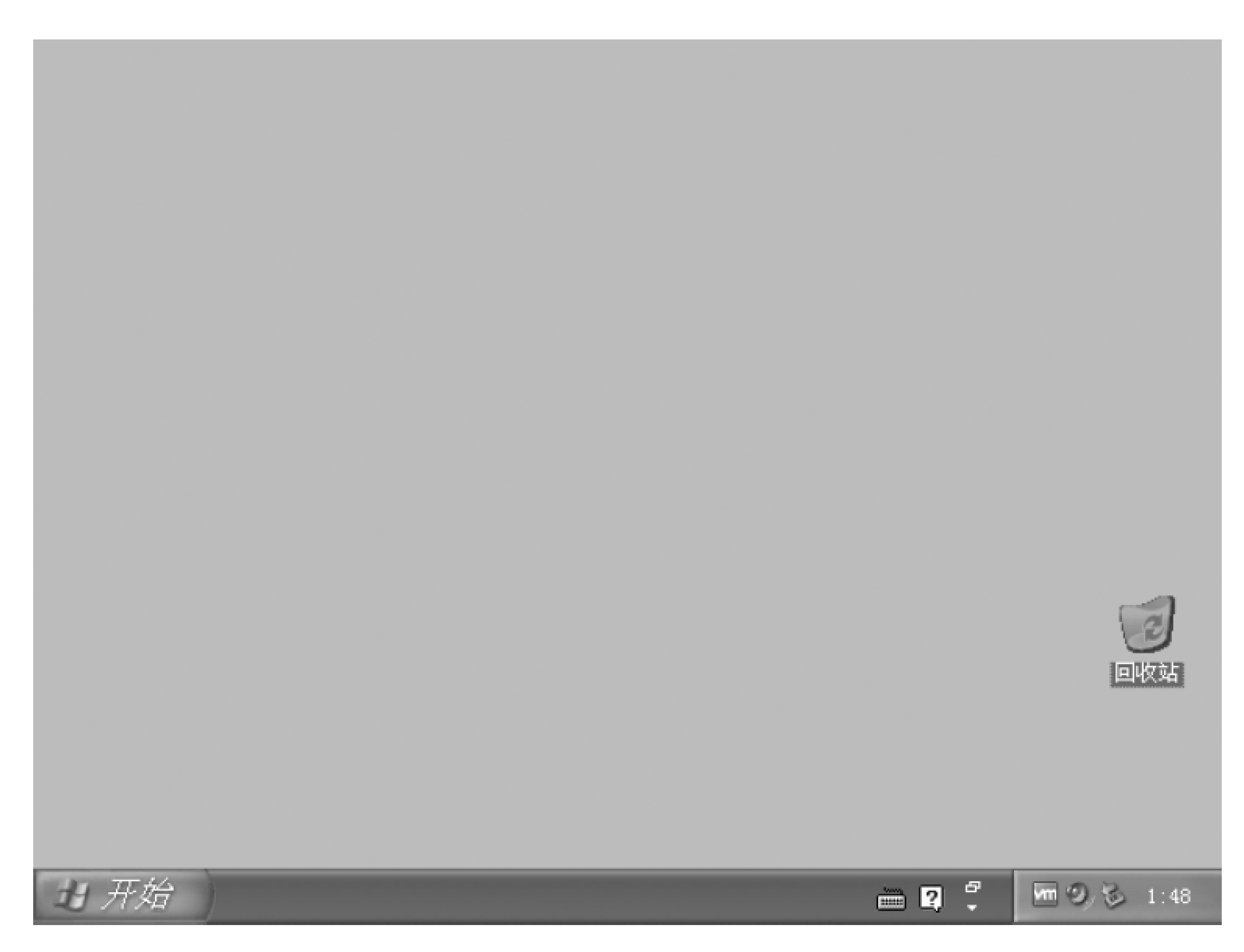


图 3-11　组策略统一设置桌面墙纸

导出收藏夹，禁用更改高级选项卡，禁用邮件快捷菜单，自定义 IE 标题栏等。这里以配置用户的收藏夹和链接为例来说明。

（1）找到"用户配置"→"策略"→"Windows 设置"→"Internet Explorer 维护"选项，如图 3-12 所示。



图 3-12　Internet Explorer 维护

（2）选择 URL，在右边的显示视图中会出现可以对 URL 配置两个选项，我们双击收藏夹和链接，这时会弹出“收藏夹和链接”对话框，如图 3-13 所示。

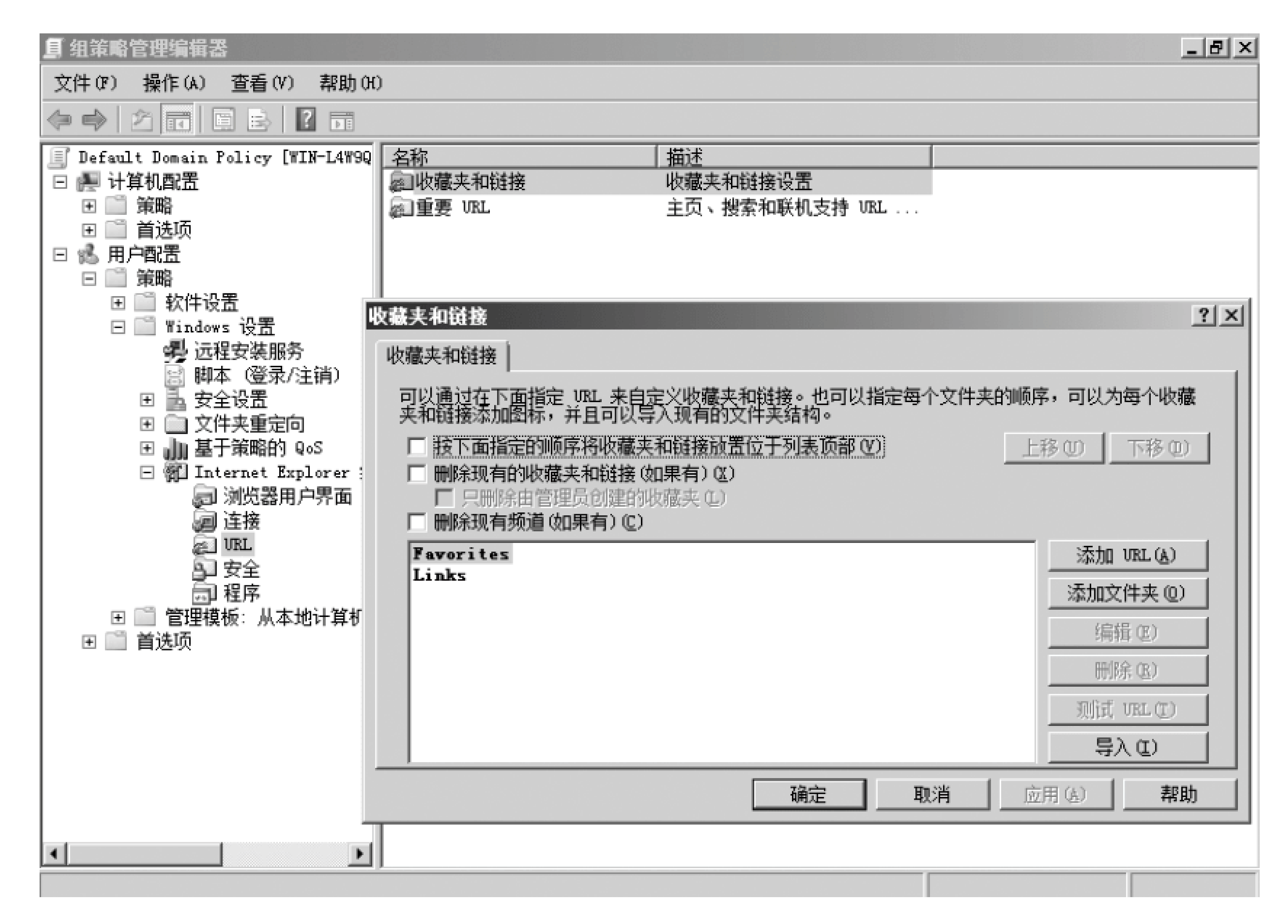


图 3-13 收藏夹和链接

（3）选中 Favorites，单击“添加 URL”，弹出“详细信息”界面，这时我们可以输入要加入的网址名称和 URL 地址。这里我们以“百度”为例，如图 3-14 所示。

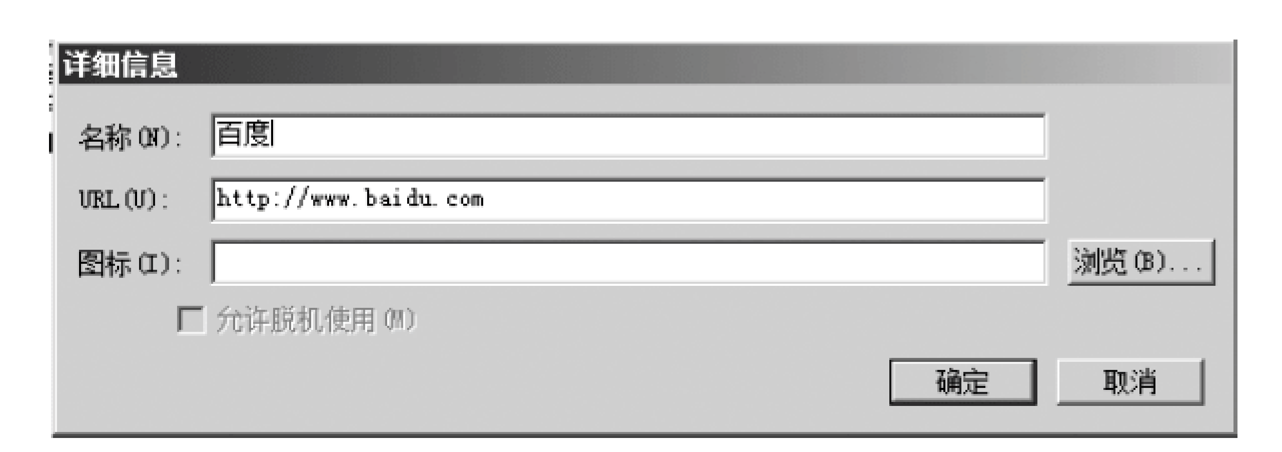


图 3-14 添加收藏夹链接

这样百度就会在用户的收藏夹中出现，进而实现了收藏夹的统一配置。

3.2.3 取消密码复杂性的要求

在 Windows Server 2008 系统中，对密码的复杂性要求较高，越是复杂的密码其安全系数就越高。但是也存在弊端，越复杂的密码越难记忆，因此很多普通用户会抱怨密码太长，很容易把密码忘记。因此在这里我们讲解管理员如何通过修改域控制器的安全策略，来取消系统中密码的负载性要求。在保证安全的前提下可以使用简单的密码，其具体操作如下。

（1）打开“组织策略管理器”对话框，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”，密码必须符合复杂性要求策略，如图 3-15 所示。

（2）双击“密码必须符合复杂性要求”，选择“已禁用”，如图 3-16 所示。



图 3-15　设置密码复杂度策略

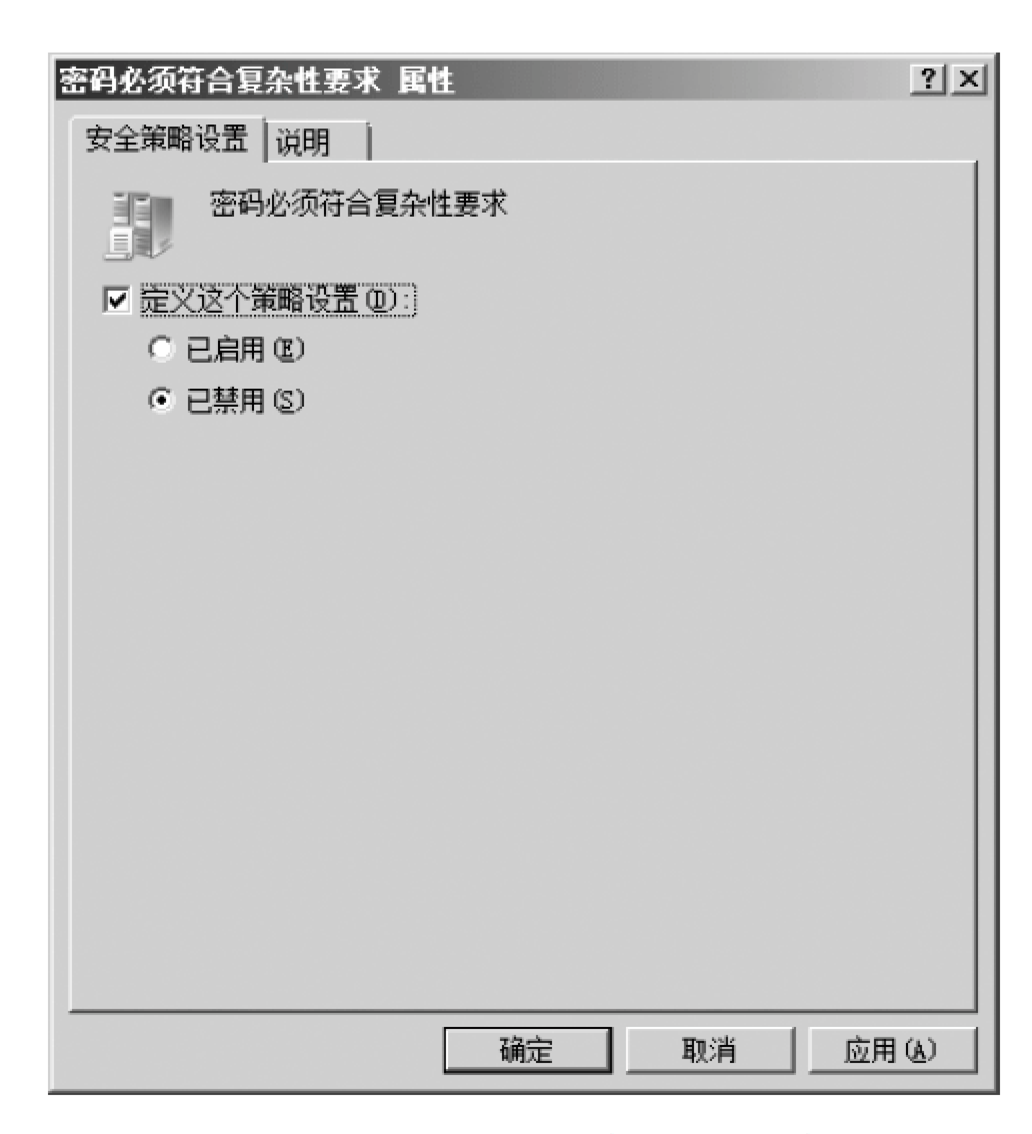
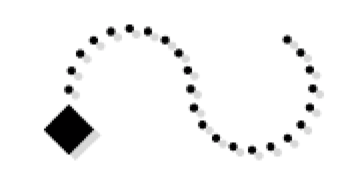


图 3-16　禁用密码复杂性要求

3.2.4　设置硬件访问控制策略

1. 可移动存储访问策略

随着移动存储设备越来越普及，移动设备的存储空间也越来越大，病毒的传播很多也可以通过移动存储进行，因此对移动设备的管理难度更是越来越复杂，伴随着出现了管理 CD 和 DVD 带来的新问题，Windows Server 2008 通过组策略可以控制对移动设备的访问和对硬件设备的安装。



（1）打开“组策略管理”窗口，右击Default Domain Policy，在快捷菜单中选择“编辑”选项，如图3-17所示。

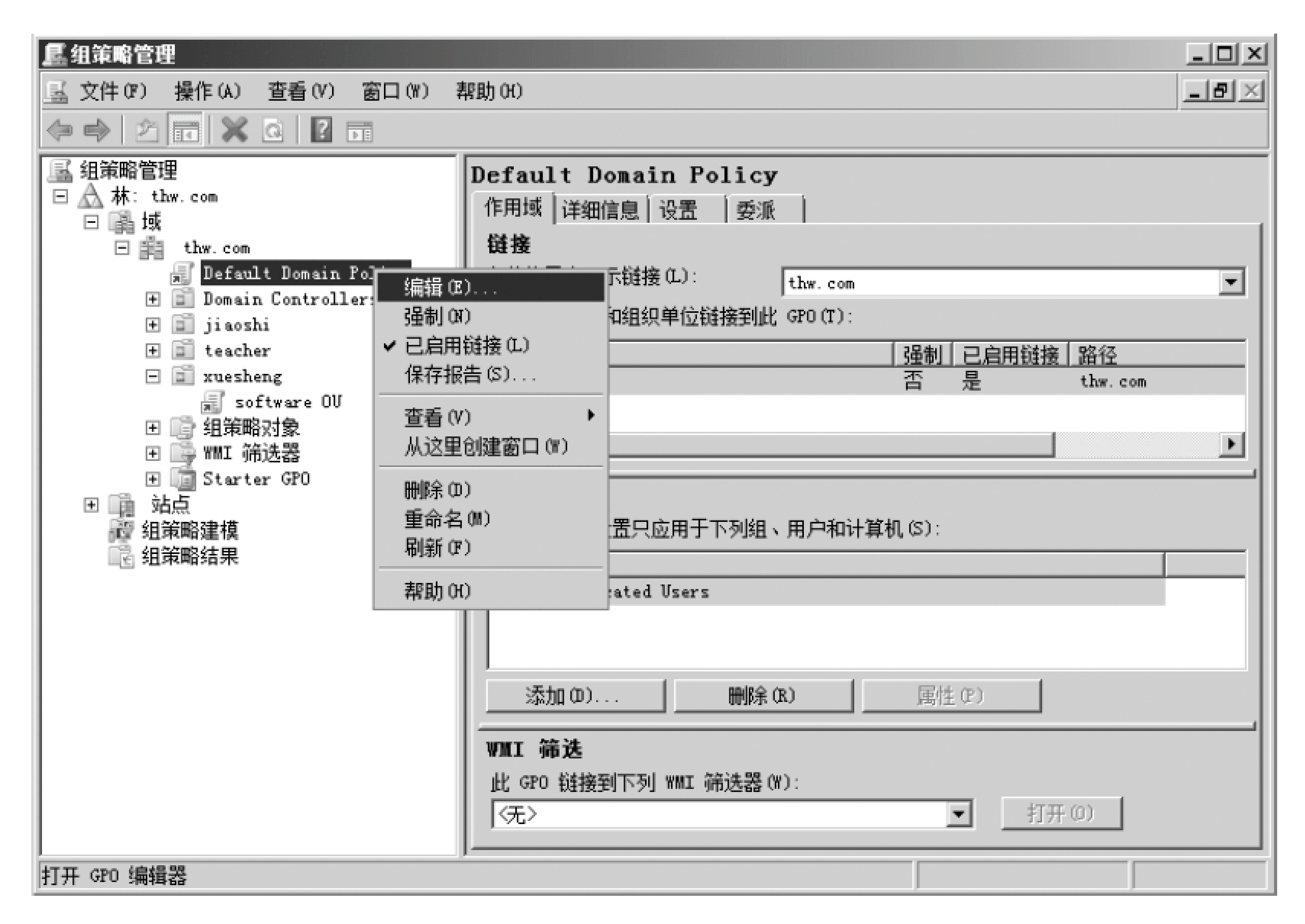


图3-17　组策略管理——Default Domain Policy

（2）单击“编辑”，弹出“组策略管理编辑器”窗口，如图3-18所示。

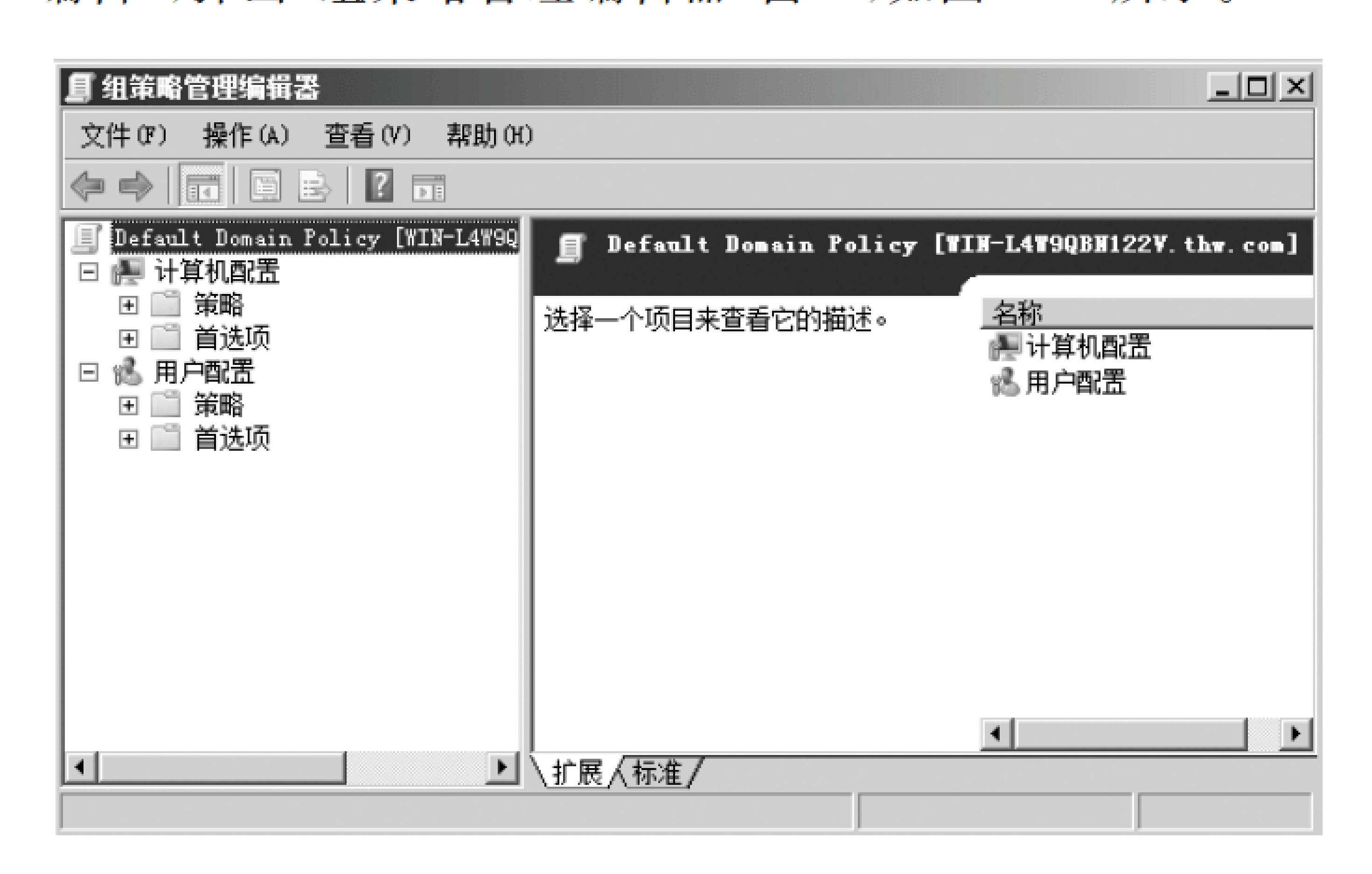


图3-18　组策略管理

（3）在“组策略管理编辑器”窗口的左侧目录树中依次选择“计算机配置”→“策略”→“管理模板”→“系统”→“可移动存储访问”选项，如图3-19所示。

（4）在“可移动存储访问”面板中，右击“CD和DVD：拒绝读取权限”策略，在快捷菜单中选择“属性”选项，显示“CD和DVD：拒绝读取权限 属性”对话框。单击“已启用”单选按钮，启用该策略。单击“确定”按钮，关闭“CD和DVD：拒绝读取权限 属性”对话框。同样的方法可以设置“CD和DVD：拒绝写入权限”策略，如图3-20所示。

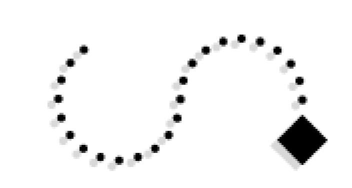




图 3-19　可移动存储访问

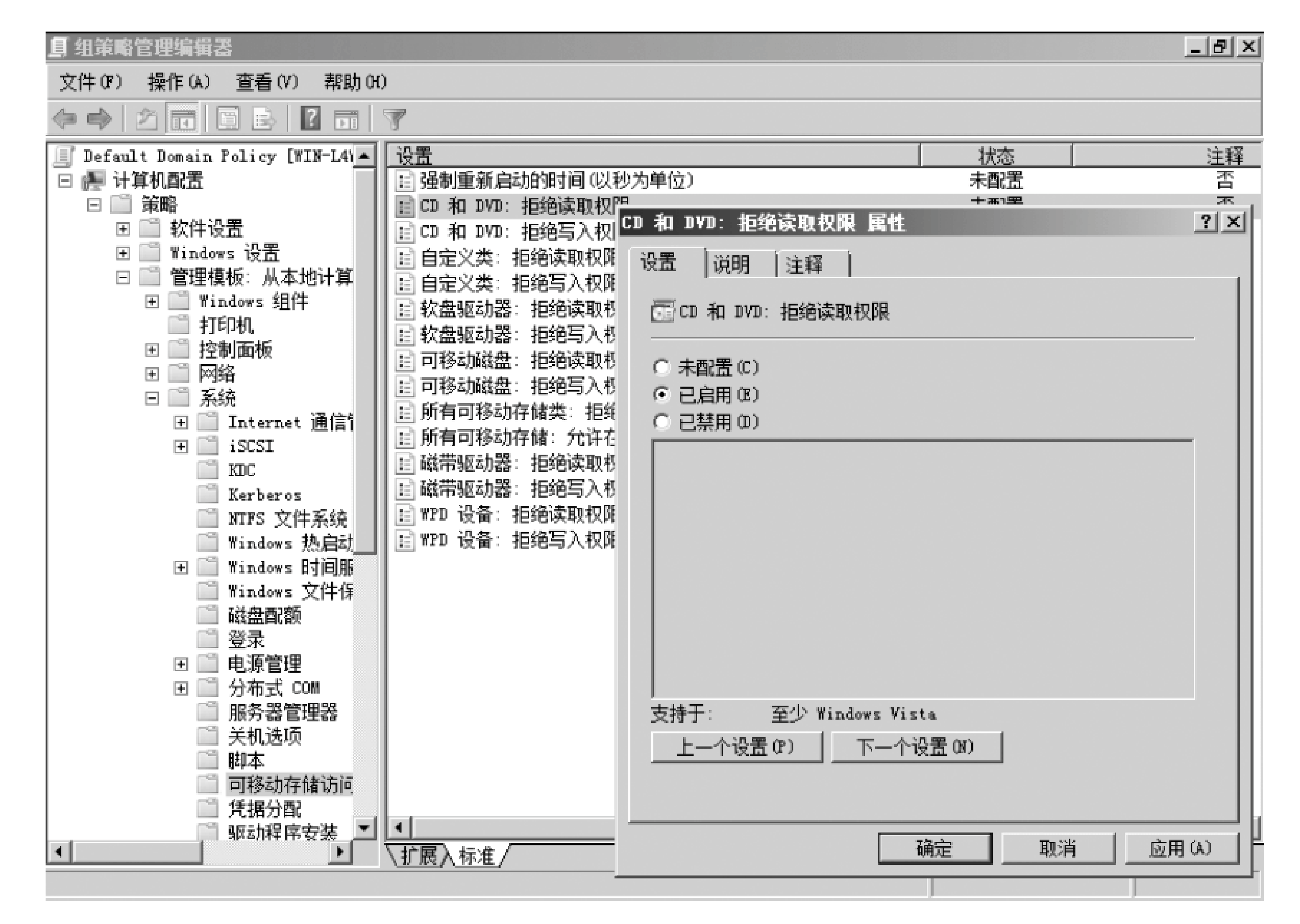
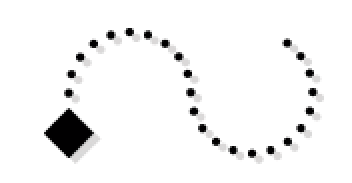


图 3-20　组策略管理编辑器——“CD 和 DVD：拒绝读取权限”策略

2. 部署“禁止安装可移动设备”策略

上述策略可以做到设备已经安装在了计算机里，我们部署了禁止访问，而这里我们部署的是不允许设备的安装。

打开“组策略管理”窗口，右击 Default Domain Policy，在快捷菜单中选择“编辑”选



项,打开"组策略管理编辑器"窗口,在组策略编辑器的左侧目录树中依次选择"计算机配置""策略"→"管理模板"→"系统"→"设备安装"→"设备安装限制"。在右侧的选项中选择"禁止安装可移动设备",出现"禁止安装可移动设备 属性"窗体,选择"已启用"单选按钮,启用该策略。如图3-21所示,此策略应用范围比较广,要谨慎使用。

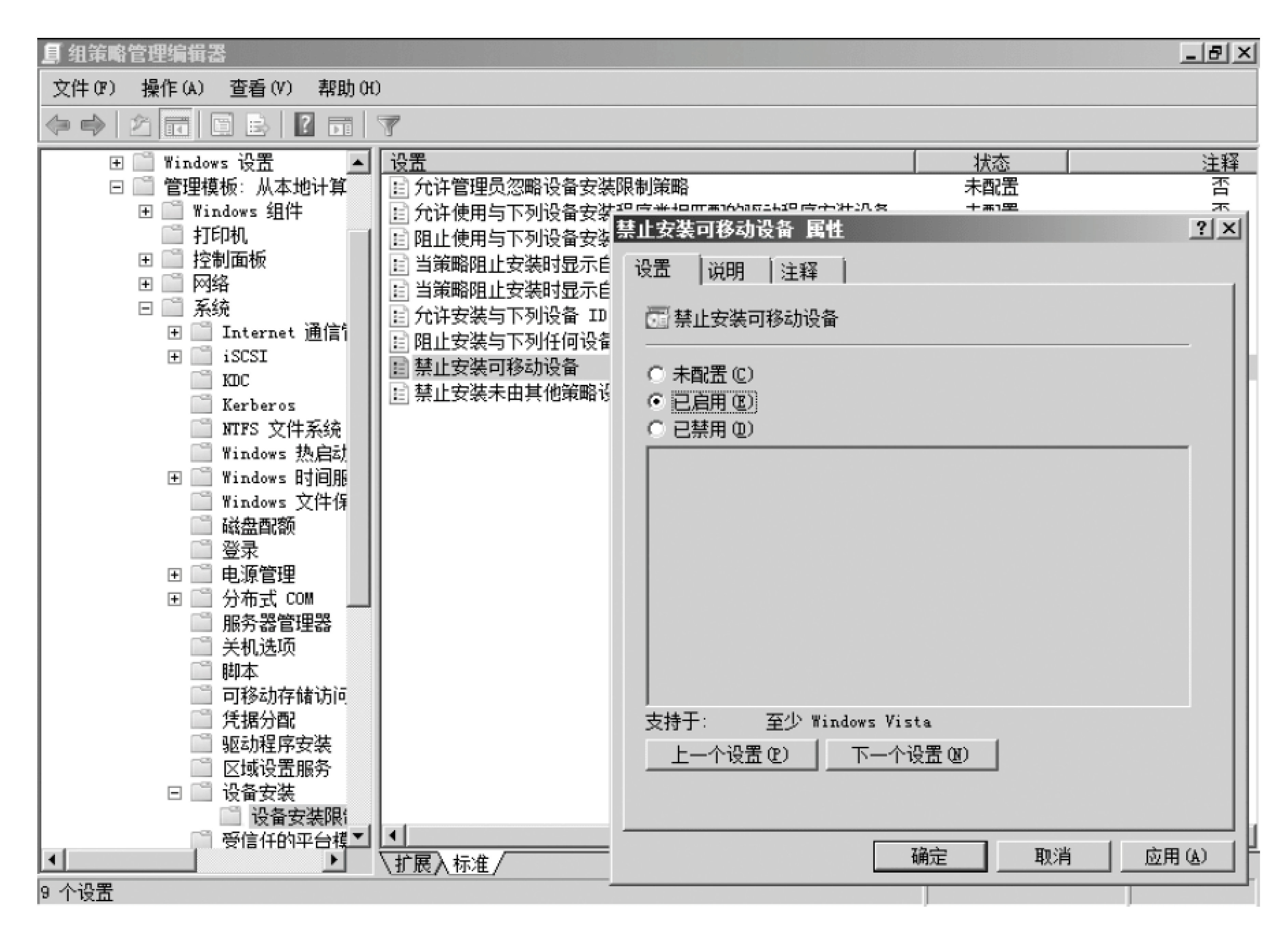


图3-21　禁止安装可移动设备

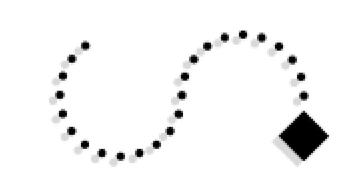
3.2.5　组策略文件夹重定向

组策略中的"文件夹重定向"功能可以把用户计算机中"我的文档"、"桌面"、"开始菜单"以及"应用程序设置"这4部分功能的文件夹从本地(C:\Documents and Settings)目录中重定向到服务器上的一个共享目录中。当然也可以扩展为我们任何想要重定向的文件夹,如QQ聊天记录,即把用户本机上的文件夹存储位置转移到域控制器上或者网络上的其他主机,从而实现对数据的统一备份与管理。

使用这个功能,我们可以实现文件夹跟随,即用户的设置与数据保存在了服务器中,无论从什么地方登录,这些文件夹都会跟随用户到所使用的计算机上。使用文件夹重定向的好处是用户在本地处理文档,处理完成之后的文档以个人名义存放在文件服务器上,而且除了本人之外的任何人都不能查看或者进行其他操作。

文件重定向的设置策略有两个选择,一个是基本,另一个高级。基本策略是将每个账户的文件夹重定向到同一位置。高级策略是指为每个组指定不同的具体重定向。

文件夹重定向的安全策略有以下两种:第一是授予用户的独占权限。若选中这个选项的话,只有用户自己对自己的文件夹具有完全控制的权限,包括系统管理员在内的其他用户都没有任何访问的权限,包括查询、修改、删除等。第二是对原有文件的管理。若选



中此项就会将原文件夹内的文件也移动到重定向后的文件夹内。

下面我们进行文件夹重定向的操作。

(1) 在文件服务器上新建一个文件夹，并把这个文件夹设置为共享文件夹，共享的权限是每个人都有完全控制的共享权限，如图 3-22 所示。



图 3-22　建立共享文件夹

(2) 在域控制器上通过组策略管理工具，编辑组织单位 caiwu 的文档文件夹的重定向，如图 3-23 所示。

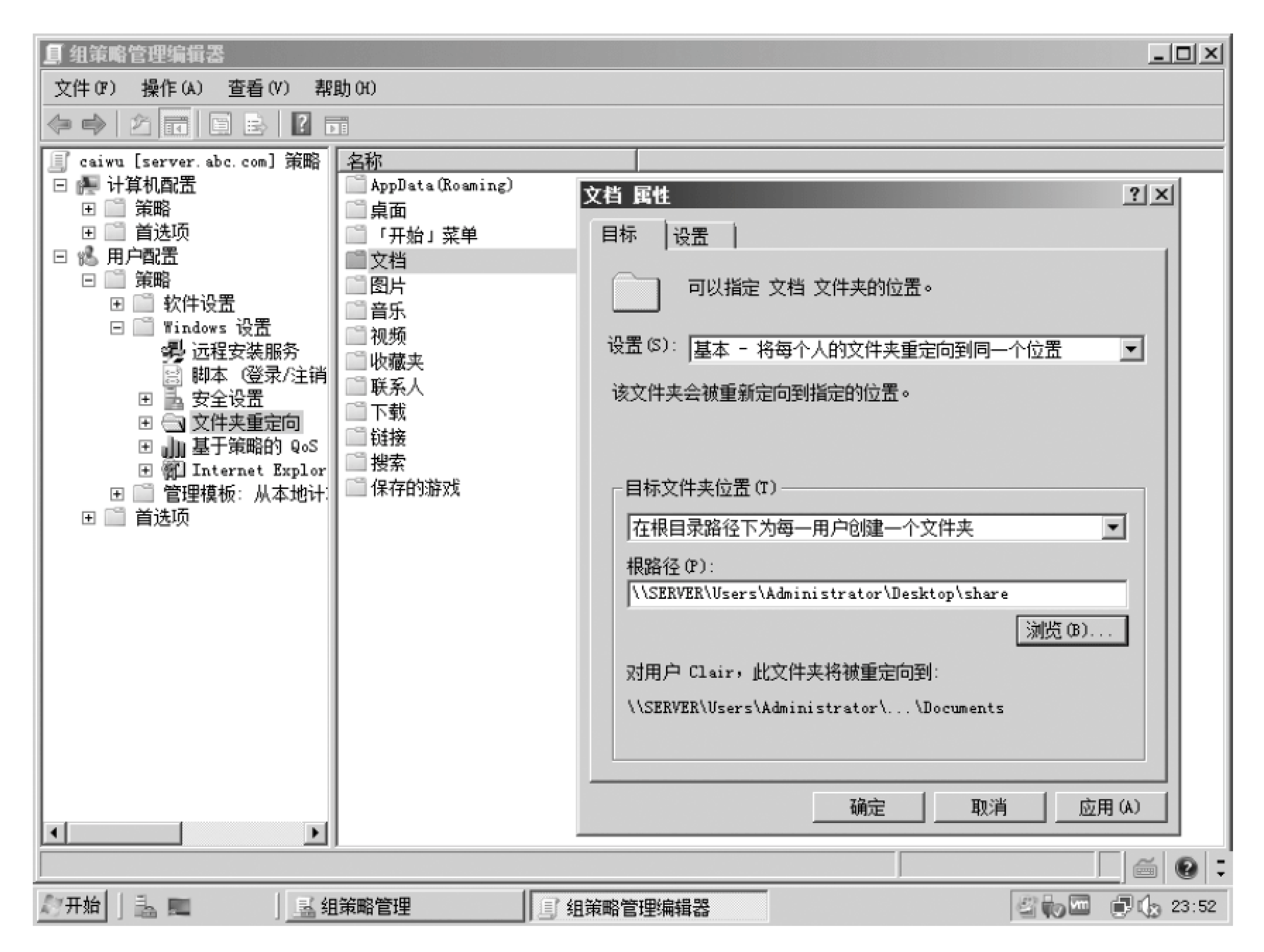


图 3-23　文件夹重定向设置

（3）以组织单位用户 zlq 身份在客户机上登录。可以看到在根目录上已经建立了文档文件夹的重定向，如图 3-24 所示。



图 3-24　在客户机上验证重定向设置

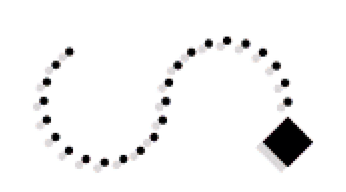
3.3　禁止程序在网络环境下的执行

3.3.1　网络环境下禁止程序运行概述

在网络应用中经常会有一些要求，如禁止某些用户运行某个程序，更特殊的要求是这些用户无论在哪个计算机上登录，禁止程序运行要求都成立。这给网络管理员提出了一个难题，本节将介绍用组策略进行管理的方法。

（1）在禁止程序运行上有下述几种方法。

- 证书规则：软件限制策略可以通过其签名证书来标识文件。证书规则不能应用到带有.exe 或 .dll 扩展名的文件。它们可以应用到脚本和 Windows 安装程序包。可以创建标识软件的证书，然后根据安全级别的设置，决定是否允许软件运行。
- 路径规则：路径规则通过程序的文件路径对其进行标识。由于此规则按路径指定，所以程序发生移动后路径规则将失效。路径规则中可以使用诸如%programfiles%或%systemroot%之类的环境变量。路径规则也支持通配符，所支持的通配符为 * 和?。相对其他规则而言，此规则设置更为灵活方便。
- 哈希规则：哈希值是通过散列算法生成的唯一标识程序或文件的一系列定长字



节。需要特别注意的是，对文件进行的任何篡改都将更改其哈希值并允许其绕过限制。但是重命名或者移动操作不会对哈希值产生影响。

- 网络区域规则：该规则主要用于使用 Windows Installer 技术安装的软件，因为通过该规则，我们可以对来自不同 Internet 区域的软件的安装程序采取不同的限制措施。

(2) 在默认情况下，系统默认为我们提供了以下常用的安全级别。

- 不允许：不允许软件运行。此级别不包含任何文件保护操作。只要用户具有修改该文件的权限，即可对一个设定成“不允许”的文件进行读取、复制、粘贴、修改、删除等操作，组策略不会进行阻止。
- 不受限：允许软件在登录到计算机的用户的完全权限下运行。此级别不等于完全不受限制，只是不受软件限制策略的附加限制。事实上，“不受限的”程序在启动时，系统将赋予该程序父进程的权限，该程序所获得的访问令牌决定于其父进程，所以任何程序的权限将不会超过它的父进程。
- 基本用户：允许程序访问一般用户可以访问的资源，但没有管理员的访问权。基本用户仅享有“跳过遍历检查”的特权，并拒绝享有管理员的权限。

(3) 对同一个软件可以应用几个软件限制策略规则。这些规则将以下列优先权顺序应用(从高到低)：哈希规则＞证书规则＞路径规则＞网络区域规则。

例如，如果某个软件程序所驻留的文件夹被指派了具有“不允许的”安全级别的路径规则，则在为该程序创建了具有“不受限的”安全级别的哈希规则后，该程序将能运行。哈希规则比任何路径规则优先级都要高。

如果对同一对象应用了两个路径规则，则两者中更为具体的规则将具有优先权。例如，如果 C:\Windows\有一个具有“不允许的”安全级别的路径规则，而 C:\Windows\System32\有另一个具有“不受限的”安全级别的路径规则，则更为具体的路径规则将获得优先权。因此，C:\Windows\中的软件程序无法运行，而 C:\Windows\System32\中的程序将运行。

如果对软件应用了两个仅在安全级别方面不同的规则，按最受限制的规则为准。例如，有两个哈希规则，一个具有“不允许的”的安全级别，一个具有“不受限的”的安全级别，当它们应用于同一软件程序时，具有“不允许的”安全级别的规则将获得优先权，因此该程序将不运行。另外，对于路径规则，总的原则就是：规则越匹配越优先。

3.3.2　网络环境下禁止程序运行的操作

这里我们以禁止组织单位(caiwu)内的用户运行 cmd. exe 为例来说明。

(1) 选择“开始”→“策略”→“管理工具”→“组策略管理”，在组织单位 caiwu 处单击，出现如图 3-25 所示的界面。

(2) 单击“编辑”命令，在“软件限制策略”处右击，出现如图 3-26 所示的界面。

(3) 单击“创建软件限制策略”，将安全级别设置为默认安全级别不受限，如图 3-27 所示。

(4) 选择其他规则，在空白处单击，选择新建路径规则，如图 3-28 所示。同时在路径处，输入 cmd. exe 的具体路径。单击“确定”，完成路径设置。

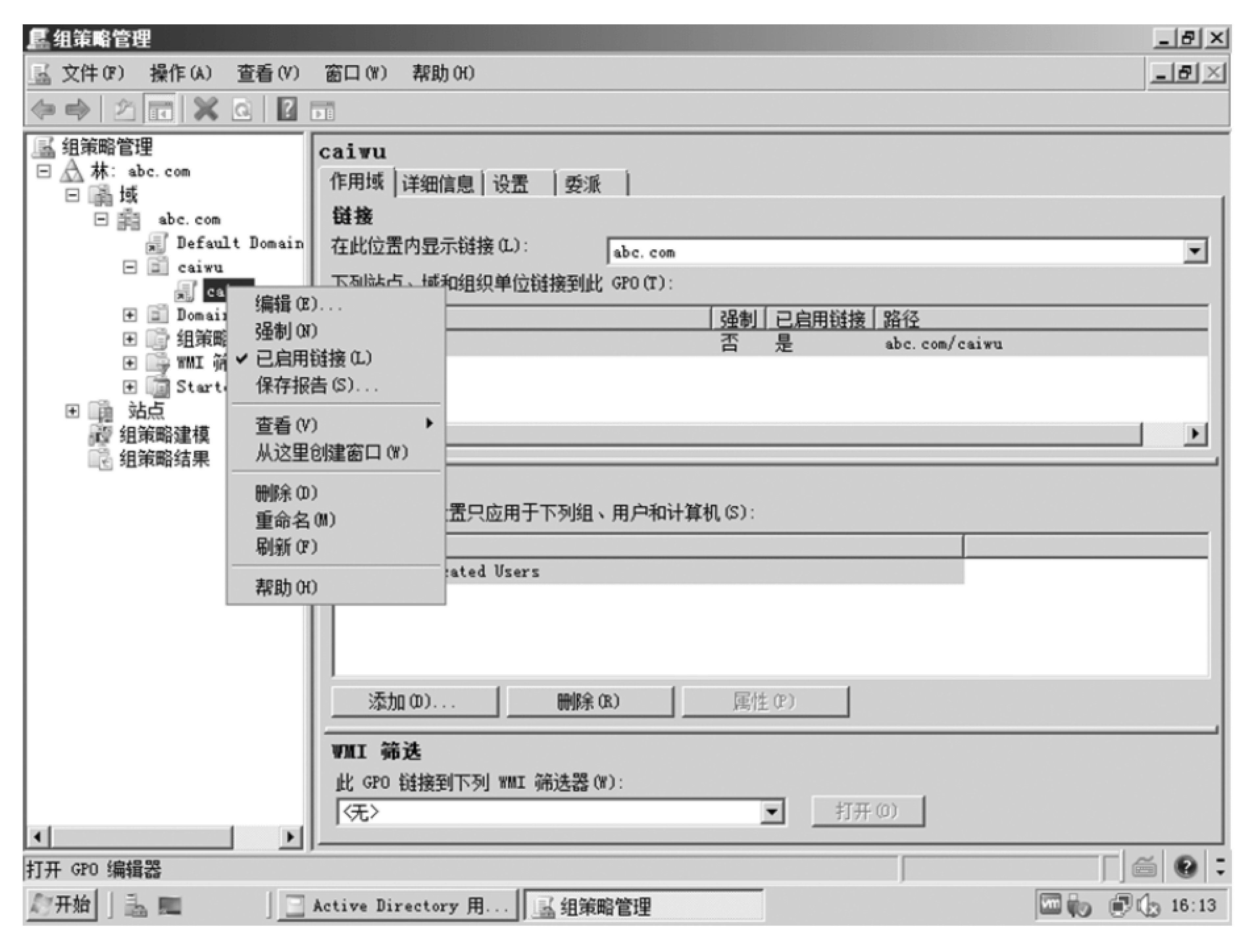


图 3-25　右击 caiwu

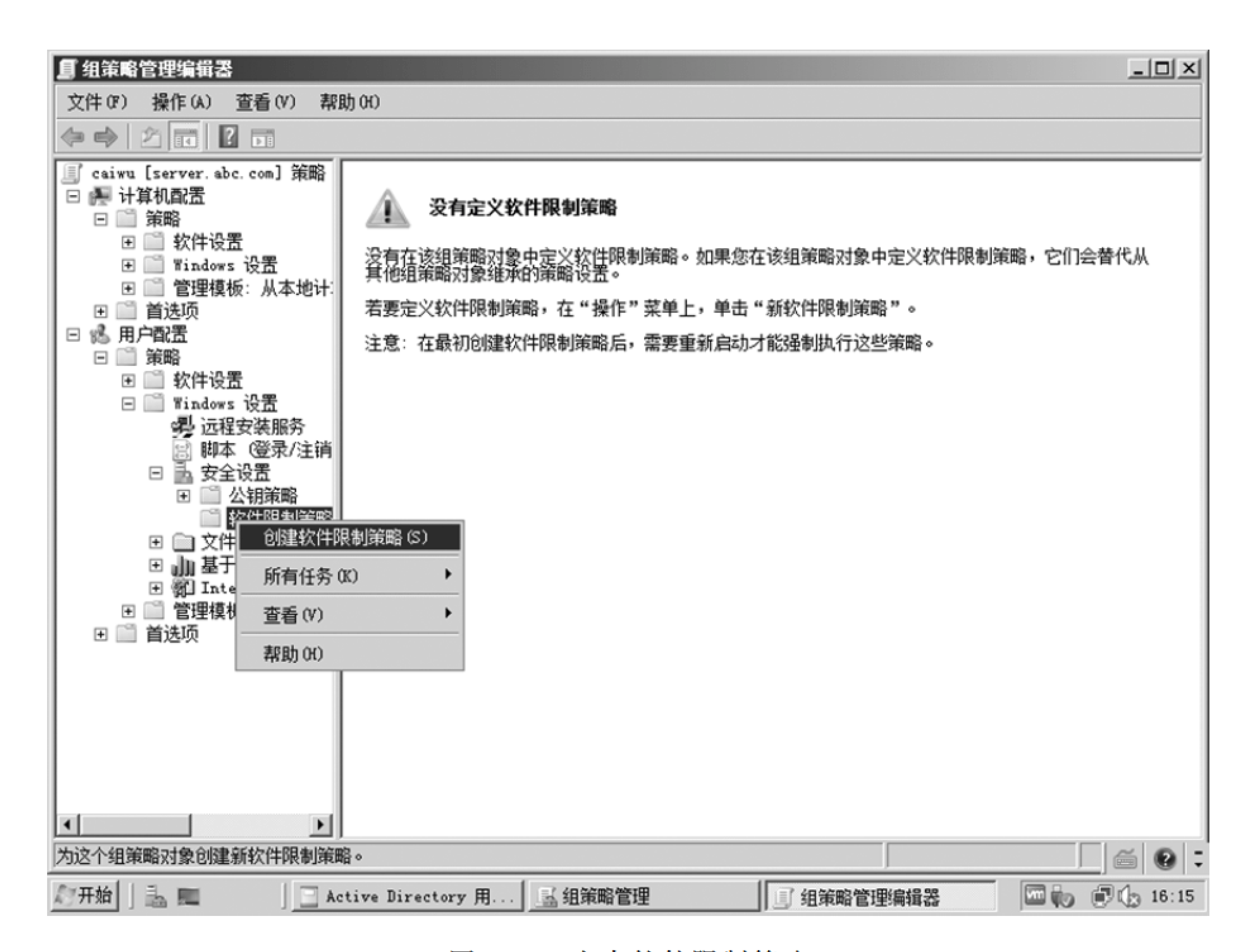
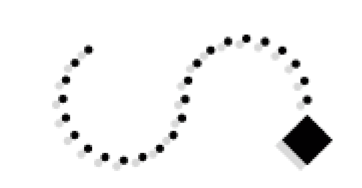


图 3-26　右击软件限制策略



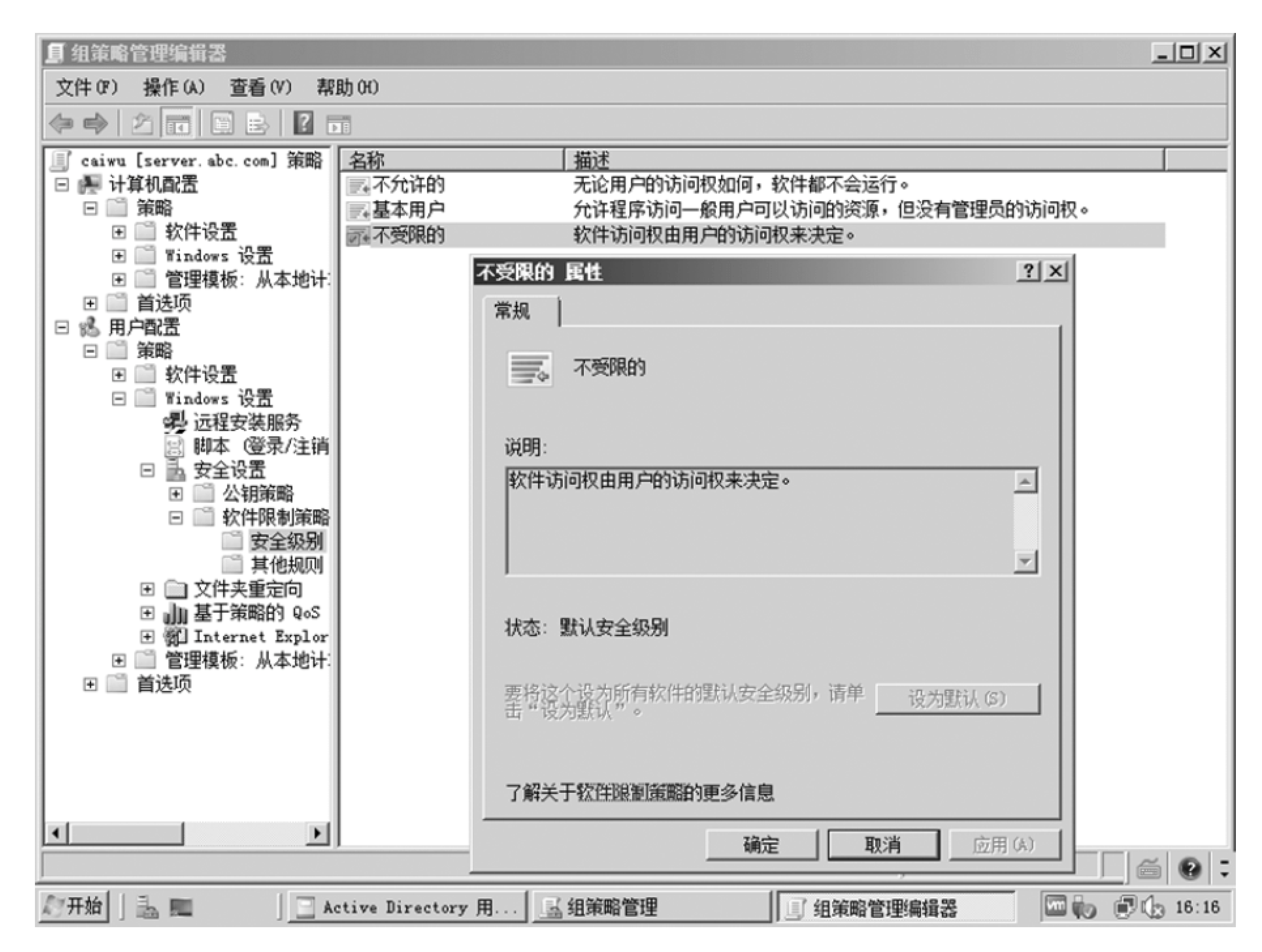


图 3-27　设置软件限制策略的安全级别



图 3-28　新建路径规则

（5）在加入域的客户机上，以组织单位 caiwu 的用户身份登录。在开始菜单的运行栏内输入 cmd.exe，按回车键出现如图 3-29 所示的用户验证界面。

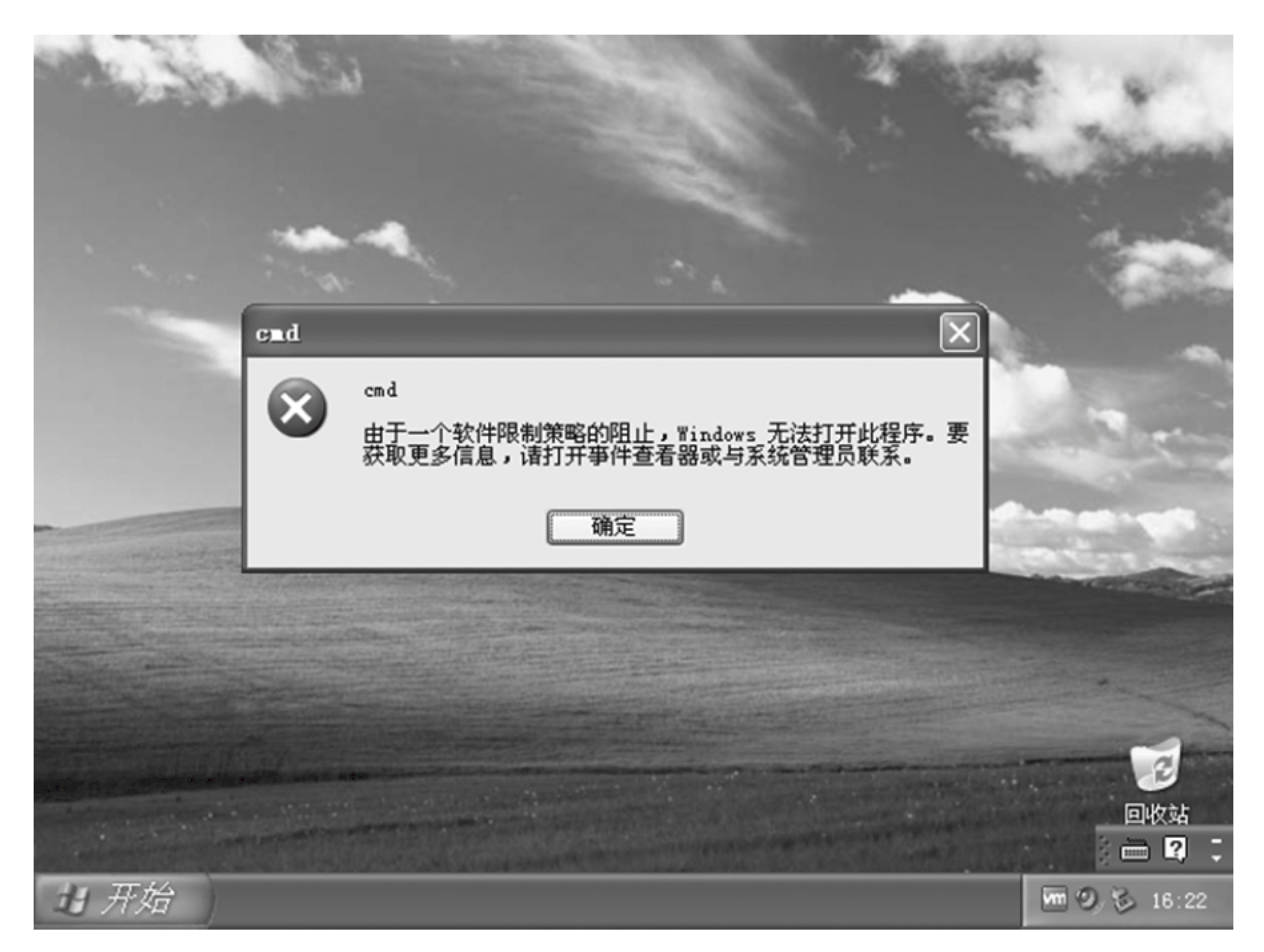


图 3-29　用户验证界面

3.4　软件远程部署

3.4.1　软件远程部署方法

在网络环境中安装软件是件很烦琐的事情，而在域环境下组策略提供了一个简单有效的解决办法，它提供了两种安装方式。

- 发布：当一个软件发布给用户，组策略生效后，用户在任何一台域中的计算机登录，所部署的软件并没有真正安装或修改客户机设置，而是出现在“添加/删除程序”中。这时并没有更改用户计算机的任何配置，也没有在“开始”菜单或是桌面上创建任何快捷方式。用户只能在“添加/删除程序中”自主决定是否安装或者删除。如果用户选择安装，软件就会自动从服务器上下载并安装到用户所在的计算机中。
- 分配：当用户计算机下一次启动的时候会自动下载并安装软件，在出现登录对话框的时候，软件已经安装完毕，这时软件才真正安装到了用户的计算机中，不仅仅是通知而已，并且只有管理员权限的用户才允许删除该软件。但是用户还是可以使用“添加/删除程序”对话框来对这个软件进行修复或者重新安装。如果用户分发的是 ZAP 文件格式的数据，则此项为虚灰色。

3.4.2　程序的远程部署操作

（1）在发布软件前，要在域服务器上建立一个共享文件夹“共享”，将安装文件使用的MSI 数据包复制到此文件夹内，并且设置相应的访问权限，注意至少要具备读取的权限。其次要配置客户端和域用户，客户端计算机我们使用 Windows XP 操作系统，同时要确定 Windows 2008 系统已经启用了网络发现和文件共享功能，如图 3-30 所示。

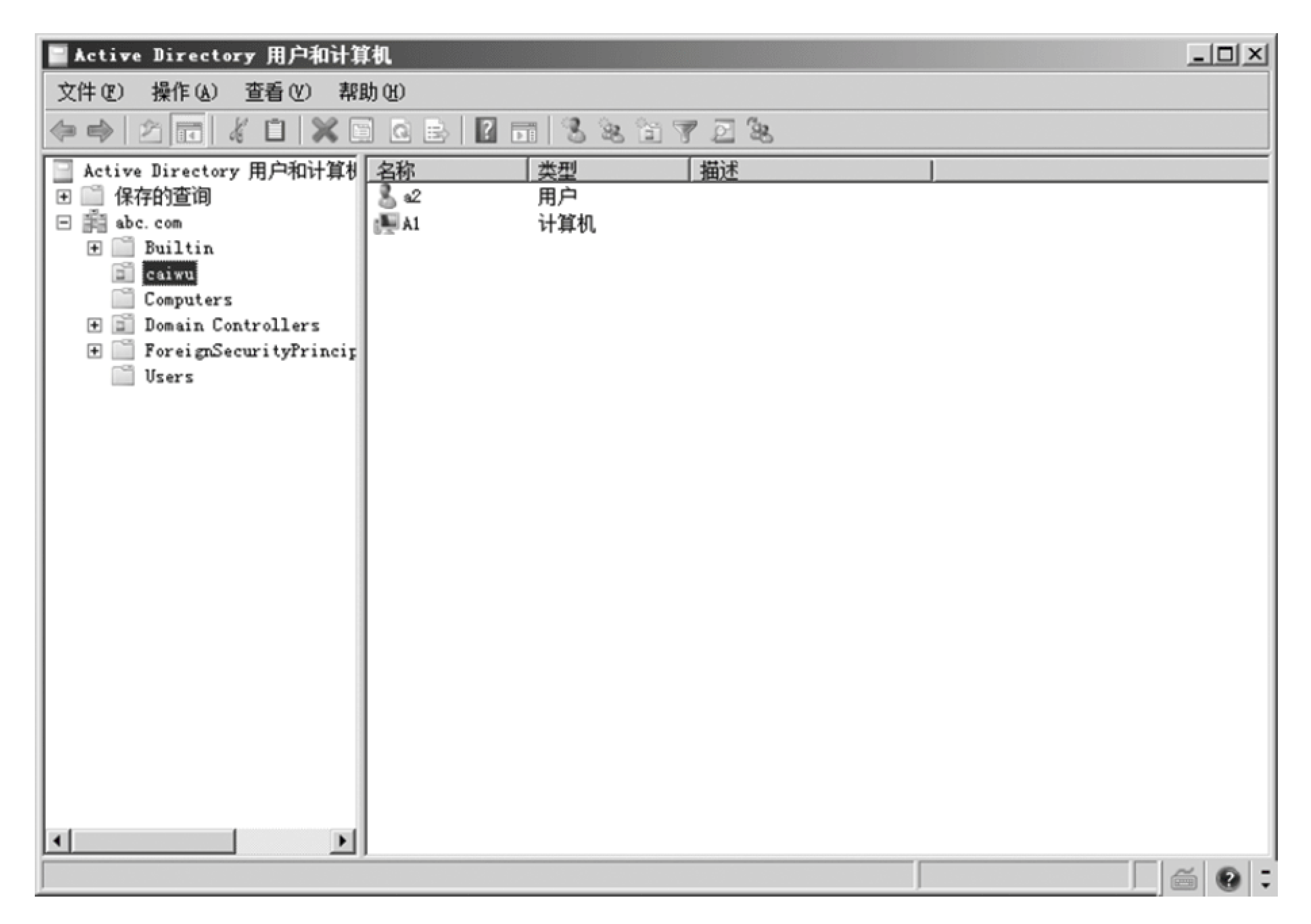


图 3-30　组织单位 caiwu 的设置

（2）在域服务器上以管理员身份登录，在组策略管理编辑器选择已经创建的名称为 caiwu 的组策略，进入组策略管理编辑器，依次选择“用户配置”→“策略”→“软件设置”→“软件安装”，右击“软件安装”并选择“属性”，如图 3-31 所示。

（3）单击“属性”。通过浏览选择要安装的软件，单击“确定”，完成设置，如图 3-32 所示。

（4）右击“软件安装”，在弹出的快捷菜单中依次选择“新建”→“数据包”，如图 3-33 所示。

（5）选择要进行发布的文件，注意这里要进行文件发布的路径必须是网络路径，共享文件位置可以是本地计算机，也可以是网络上任何一台设备，但是要有足够的访问权限，如图 3-34 所示。

（6）右击新建的数据包，在快捷菜单中选择“属性”选项，打开软件发布包的属性对话框。在“部署”选项卡中进行部署类型的设置，如图 3-35 所示。

（7）在客户机上，以 caiwu 的身份登录，打开控制面板中的添加新程序，即可看到通过网络部署的程序，如图 3-36 所示。



图 3-31　选择软件安装属性

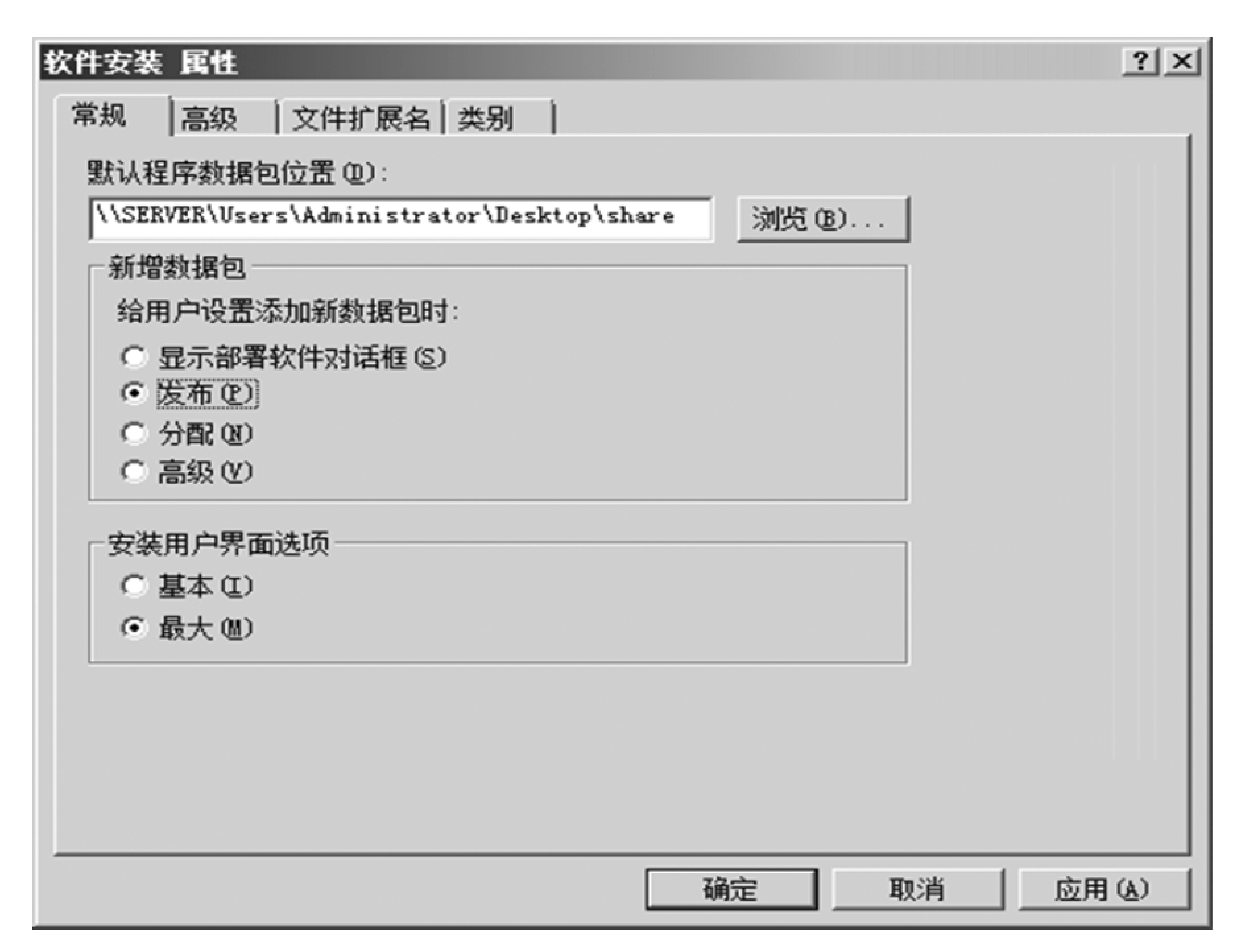


图 3-32　完成属性设置

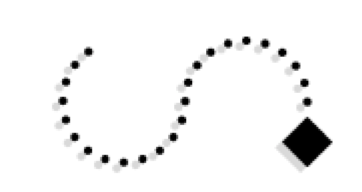




图 3-33 选择新建数据包

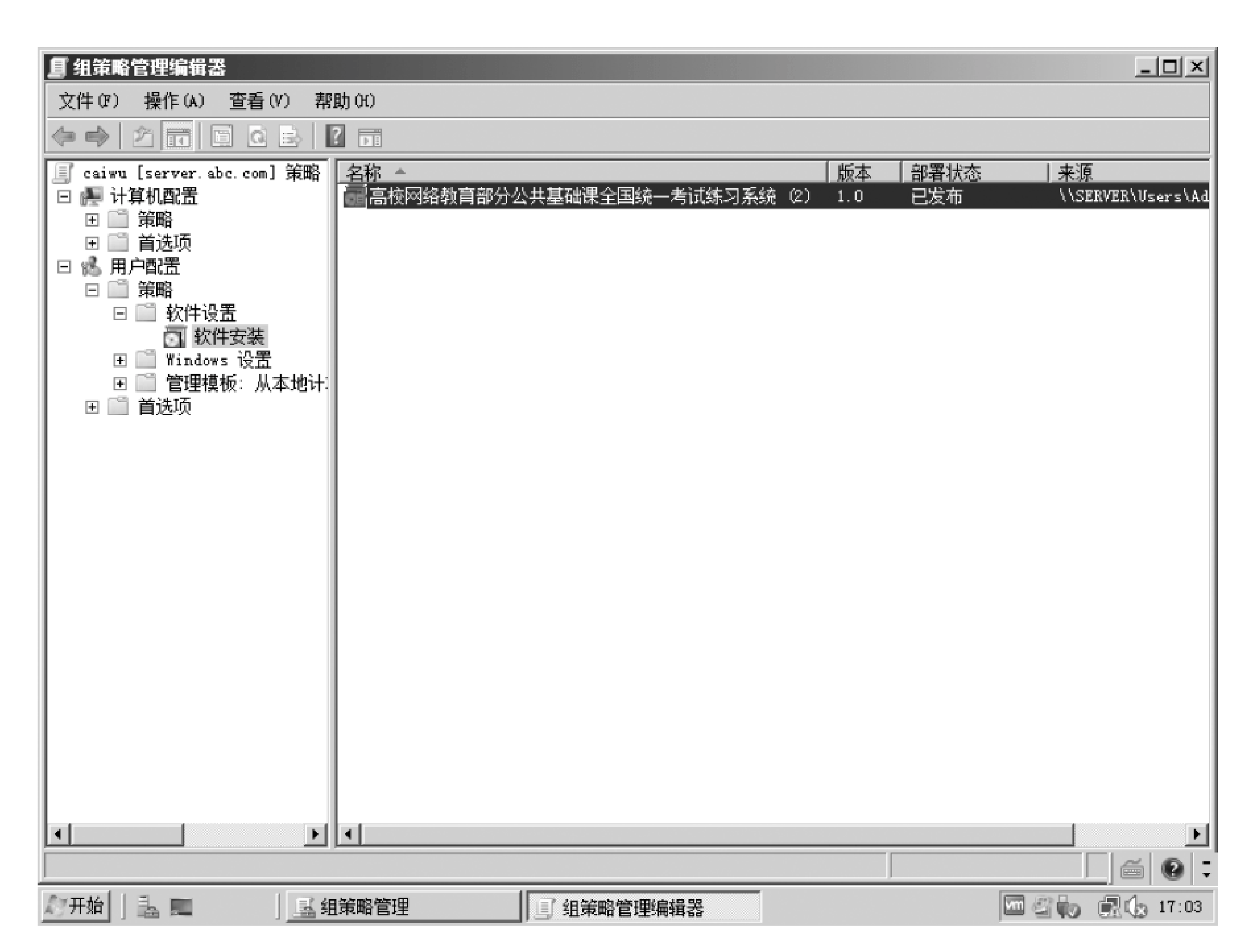


图 3-34 选择要进行发布的文件

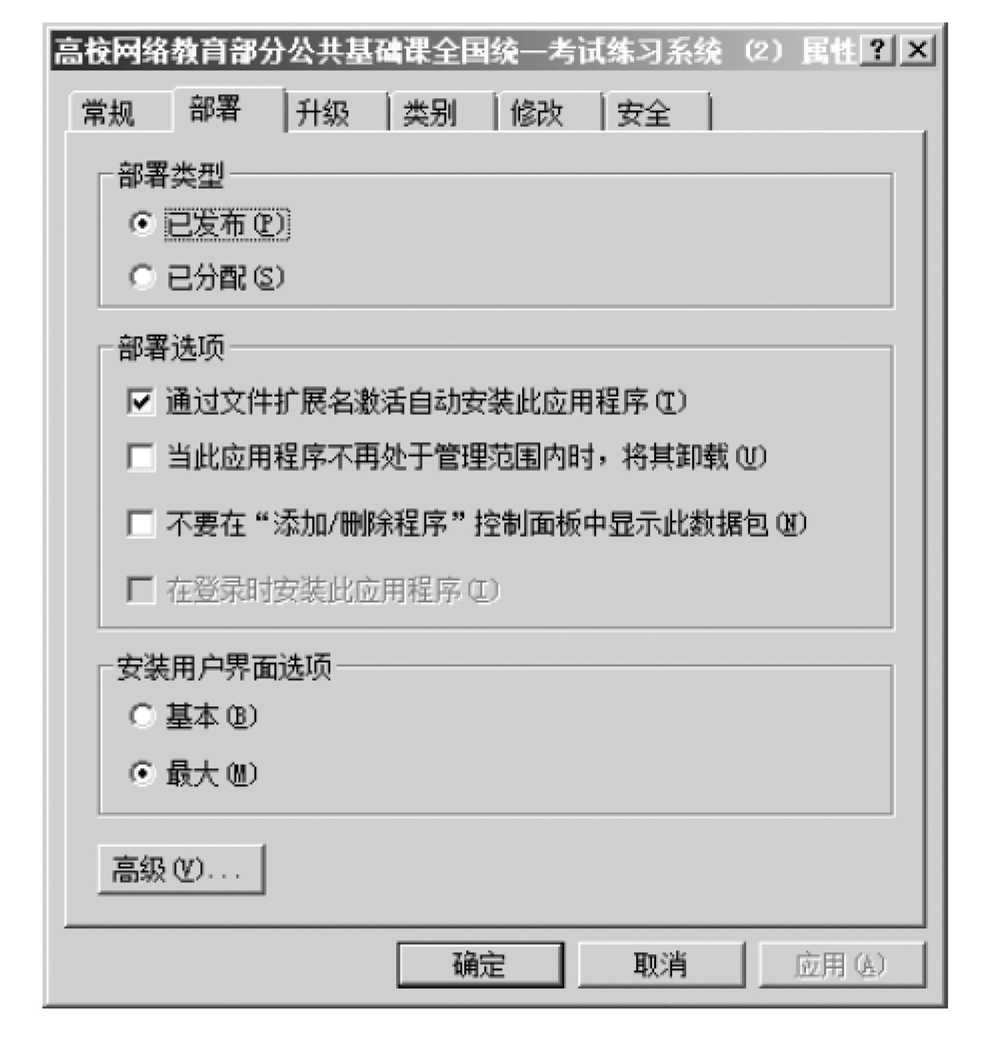


图 3-35　设置部署选项卡



图 3-36　以用户身份登录验证安装

本章小结

本章介绍了在活动目录中基于组策略的管理方法。重点讲解了组策略的功能、管理与维护方法，同时介绍了如何用组策略进行个性化设置和网络环境下程序的管理方法与操作技巧。通过学习要求掌握组策略的功能、内容、管理与维护方法。掌握用组策略进行桌面设置、收藏夹和链接、文件夹重定向和硬件访问策略的设置方法与操作要点。掌握通

过组策略进行程序的远程安装和禁止运行的技术和操作技巧。另外还需要了解第 1 章中关于组策略的相关内容，以便形成对组策略的完整理解与认识。

本章习题

1. 简述组策略的功能与内容。
2. 简述软件的部署方式和禁止程序运行的方法。
3. 禁止某单位行政组计算机运行 Outlook Express。
4. 只允许某单位服务组用户运行 Microsoft Office。
5. 实现 Office 的自动安装。

第4章

SNMP

【本章重点】

本章要求掌握网络管理的基本概念，理解管理信息库的基本知识和 SNMP 的协议单元格式及操作，了解远程网络监控的知识。如果学时较少，可只学习 4.1 节，有关 SNMP 的内容不进行学习。

计算机网络最初发展时，网络设备的数目很少，网络管理员只需要 Ping 每台计算机，并通过自动返回的信息就可以判断网络是否出了故障。当计算机网络向全球蔓延，并最终形成全球化的 Internet 时，已有成千上百家网络设备厂商生产出了几万种不同的网络设备，计算机网络的管理成了巨大的难题。为了解决网络管理与维护，如何对网络进行有效的管理变成我们研究的问题。

4.1 网络管理协议概述

在网络构建过程中，大量不同型号、不同生产厂家的设备要混合使用，不同类型的网络之间要互相联通，这就需要网络管理系统提供一个统一的、全面的接口，并达到以下目标：

- 具有统一的协议和服务，以便管理信息可以保持一致性。
- 对网络性能、安全、配置、计费和故障等方面有标准的定义。
- 允许增加新的应用与服务。
- 减少不同系统之间交换信息的费用。

1979 年，国际标准化组织（ISO）开始对网络管理的标准化进行研究，随后国际电报电话咨询委员会（CCITT）也参与了这项研究。1989 年 ISO 颁布了 ISO DIS7498—4（X.700）文件，其定义了网络管理的基本概念和总体框架。1991 年，ISO 又颁布了公共管理信息服务即 CMIS（ISO 9595）和公共管理信息协议即 CMIP（ISO 9596）。CMIP 是在 TCP/IP 的 SNMP 的基础之上设计的。

CMIP 采用了面向对象的技术，不仅有数值属性，而且有行为属性，是一种真正的面向对象的技术。但是相对于 SNMP 而言，CMIP 的实现需要大量资源，因此 CMIP 没能

流行起来。1992 年 ISO 公布了系统管理功能即 SMF（ISO 10164）和管理信息结构即 SMI（ISO 10165），这些文件共同组成了 ISO 的网络管理标准。虽然 ISO 制定的标准非常强大，但也非常复杂，因此目前有关 ISO 管理的实现非常缓慢。

随着 Internet 的迅速发展，有关 TCP/IP 网络管理的研究活动十分活跃，相关的网络管理标准也被广泛应用，成为事实上的标准。TCP/IP 网络管理标准称为简单网络管理协议（SNMP），其公布在 1990 和 1991 年的几个 RFC 文件中，即 RFC1155（SMI），RFC1157（SNMP），RFC1212（MIB 定义），RFC1213（MIB-2 规范）。由于 SNMP v1 过于简单，造成系统不够安全和管理上的不完善。几年后产生了简单网络管理协议第二版（SNMP v2），其定义在 RFC1902～RFC1908 文档中。SNMP v2 组合了 RMON 等内容，使得 SNMP 在安全和性能方面都有了提高。

除了上述两个网络管理标准外，还有 IEEE 定义的局域网（LAN/MAN）的管理标准 IEEE802.1b，以及 ITU-T 为了适应电信网络管理的需要在 1989 年定义的电信网络管理标准即 TMN（M.30 建议蓝皮书）等。

1. 网络管理体系结构的基本概念

对网络管理的能力进行抽象，人们提出了网络管理体系结构的概念。用于定义网络管理系统的结构及系统成员间相互关系的一套规则就是网络管理体系结构。根据网络管理体系结构的定义可知，网络管理体系结构需要研究单个网络管理系统内部的结构及其成员之间的关系，以及研究多个网络管理系统如何相互兼容并连接构成可以管理复杂网络的管理系统。在网络管理体系结构中，网络管理被抽象成一种独特的网络应用。

网络管理体系结构工作在协议的上层，这是网络管理工作的基础结构。网络管理体系结构的特点是：

- 管理功能分为管理站（Manager）和代理（Agent）两部分。
- 为存储管理信息提供关系数据库或面向对象的数据库支持。
- 提供用户接口和用户视图，如 GUI 和管理信息浏览器等。
- 提供基本的管理操作，如获取管理信息、设置参数以及警告等操作。

网络管理体系结构示意图如图 4-1 所示。

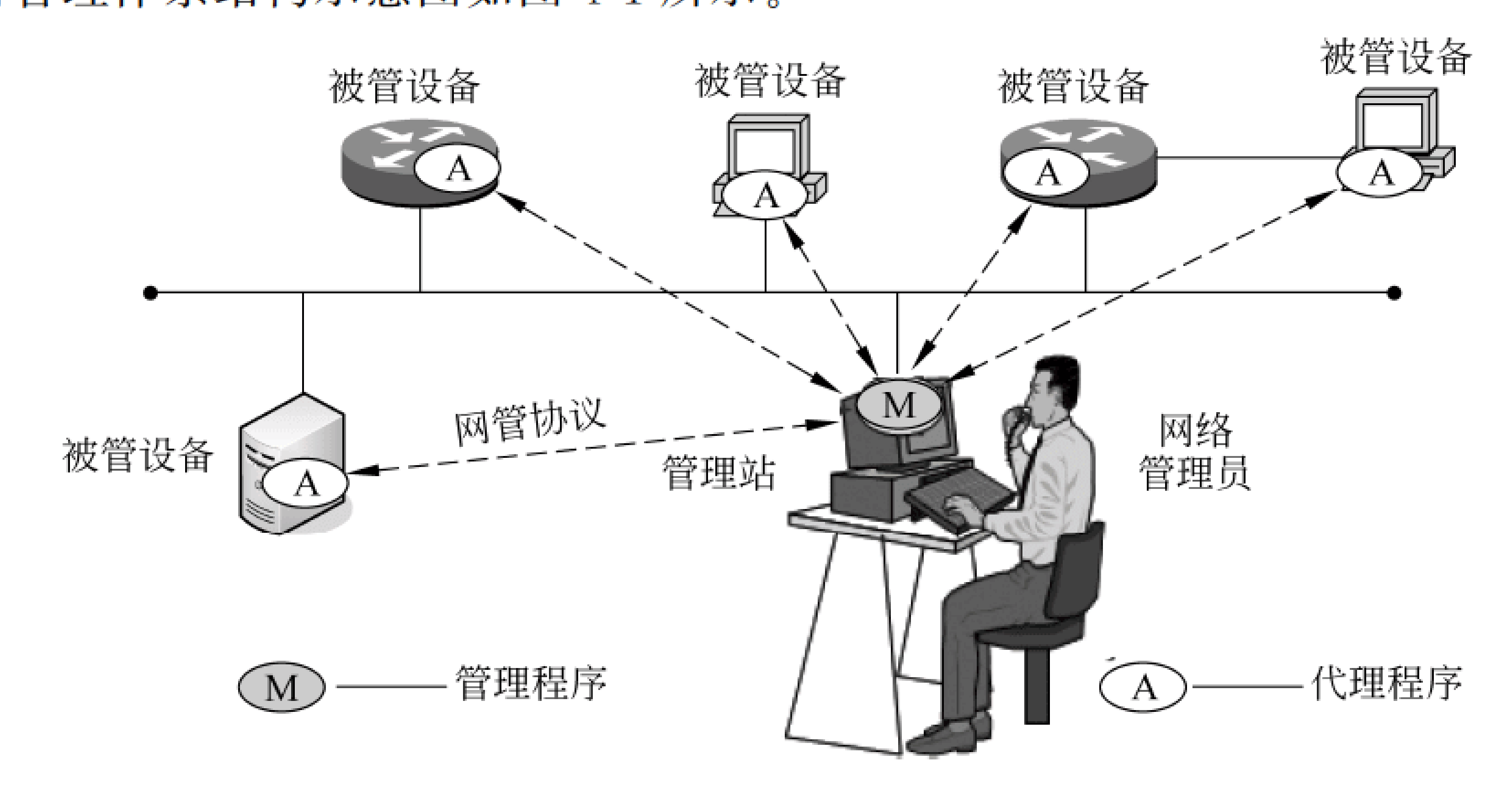


图 4-1　网络管理体系结构示意图

2. TCP/IP 网络管理体系结构

SNMP 早在 1987 年就制定，而且不断有新的协议推出，但是 SNMP 凭借其结构简单、使用方便、且与 TCP/IP 联系紧密的特点一直到今天仍然被广泛地使用。SNMP 管理体系结构由管理者(Manager)、代理(Agent)和管理信息库(MIB)三部分组成。

管理者是管理指令的发出者，这些指令包括查询和设置参数等管理操作，管理者通过各设备的管理代理对网络内的各种设备、设施和资源实施监控。代理负责管理指令的执行，并根据结果返回给管理者一些信息。代理有三个基本功能：

- 从 MIB 中读取各种变量值。
- 根据管理者的要求修改 MIB 中的各种变量值。
- 当代理设备出现问题时，以通知的形式向管理者报告被管对象发生的一些重要事件。

管理者和代理之间主要以请求/应答方式工作。管理者向代理发出请求指令，获取或者设置网络元素的参数。代理向管理员返回应答响应，报告请求的执行结果；为了使一个管理员可以管理多个代理，常采用轮询的方式。

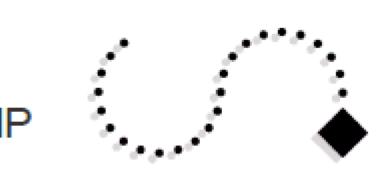
MIB 是被管对象结构化组织的一种抽象。MIB 是一个概念上的数据库，由管理对象组成，各个代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。

SNMP 是一个异步的请求/响应协议，其实体不需要在发出请求后等待响应的到来。SNMP 中包括了 5 种基本的操作：

- get-request 操作用来查询指定的网络管理对象的信息。
- get-next-request 操作用来查询指定的网络管理对象的下一个对象的信息，其还可以遍历 MIB 树并判断哪些对象存在。
- set-request 操作用来修改或创建管理对象及其信息。
- get-response 操作是由代理方发出的，所以它不是管理操作，它的作用是返回由 get、get-next 或 set 操作发出的查询或设置操作的结果。
- trap 操作也是由代理发出的，它可以查找特定的事件并检测，并向管理者通报重要事件的发生。

SNMP 在计算机网络系统中应用非常广泛，已经成为事实上的计算机网络管理标准。但是 SNMP 有许多缺点，是它自身难以克服的：

- SNMP 的最大问题是太过简单而无法处理各种细节信息，无法满足当今日益膨胀的网络的发展需要，这也是 SNMP v2 以及 SNMP v3 出现的原因。
- SNMP 不适合真正大型网络的管理，因为它是基于轮询机制的，这种方式有严重的性能问题，如不适合查询大量的数据。
- SNMP 存在一些安全管理漏洞，网络入侵者很容易获取正在通过网络传递的各种信息，甚至可以关闭某些终端。
- SNMP 的 trap 是无确认的，这样不能确保管理者接收到了非常严重的警告信息。
- SNMP 不支持如创建、删除等类型的操作，要完成这些操作，必须用 set 命令间接地触发。



- SNMP 的 MIB 模型不适合比较复杂的查询，因此没有一个标准或建议定义了 SNMP 网络管理体系结构。另外，由于定义了太多的管理对象类，当管理者需要查询或修改时，他必须明白这些管理对象类的准确含义。

4.2 管理信息库

管理信息库(Management Information Base，MIB)，是一个以层次式树状结构为组织结构的管理信息集合，所有的管理对象都分布在这个树状结构中。MIB 被 SNMP 访问和使用。

4.2.1 管理信息结构

管理信息结构(Structure of Management Information，SMI)，为命名和定义管理对象指定了一套规则。上百家厂商的产品都遵循这个规则，以使网络设备能够相互兼容。

1. ASN.1 简介

ASN.1 是抽象语法符号 1(Abstract Syntax Notation One)的简称，是一种标准的对象定义语言和编码规则。虽然它太复杂、缺点多以及运算效率不高，但是 SNMP 已经完全融进 ASN.1 了，所以要想了解 SNMP，就必须熟悉 ASN.1。

在 SNMP 上应用的 ASN.1 有一些用词上的惯例：

- 固有的数据类型一般都以大写字母表示，如 OCTET STRING。
- 用户自定义的数据类型以大写字母开头，但至少有一个非大写字母，以便与固有的数据类型区分开。
- 标识符可以包括大写字母、小写字母、数字和下划线，但必须以小写字母开头，如 internet。
- 空格、回车符和 Tab 键并不十分重要。
- 注释以字符串“--”开头，直到行尾或下一个字符串“--”出现。

ASN.1 一共有 5 种固有的基本数据类型，如表 4-1 所示为这些类型及其说明。

表 4-1　在 SNMP 中使用的 ASN.1 的基本数据类型及其说明

基本数据类型	说　明
INTEGER	任意长度的整型数
BIT STRING	一个 0 或多位比特的串
OCTET STRING	一个 0 或多位无符号字节串
NULL	位置符，表示为空
OBJECT IDENTIFIER	对象标识符类型

理论上没有规定 INTEGER 类型的长度范围，但是其他的 SNMP 规则限制了它的范围，因为实际应用中不可能出现无限大这种情况。下面列举了一个使用 INTEGER 类型的例子，用 ASN.1 定义了一个 INTEGER 类型的变量 counter 并初始化为 1。

示例如下：

```
counter INTEGER∷=1
```

有时也需要一种整型的子类型，将变量的值限定为特定的一些值或在一定的范围里，实际应用中这种情况较常见。例如，定义一个状态子类型 Status，其定义如下：

```
Status∷=INTEGER{up(1),down(2),unknown(3)}
```

定义好后，就可以应用这种子类型了。例如接口 1(Interface1)的定义。

示例如下：

```
Interface1 Status∷=1
```

BIT STRING 是比特串，其每一个比特要不是 0，要不是 1。与其相似的是 OCTET STRING(无符号字节串)类型，只不过这种类型中每一个字节的范围是 0～255。上述两种类型，可定义串的长度和初值。

NULL 表示空，或是位置符。例如在 SNMP 的 get 操作的对象标识符值域中就是 NULL 类型。

OBJECT IDENTIFIER 是一种标识管理对象的方法，这些管理对象被组织成一种树的结构存放，从树的“根”开始到每一个管理对象都有唯一的一条路径，相应地也就有唯一的一个标识。例如，定义 internet 的对象标识符。

示例如下：

```
internet OBJECT IDENTIFIER∷={iso(1) org(3) dod(6) internet(1)}
```

ASN.1 基本上是一种原始的数据声明语言，除了上述 5 种基本数据类型以外，它还允许用户自定义原语对象，然后再把它们组合成复杂的构造对象。构造类型有 4 种方法，如表 4-2 所示。

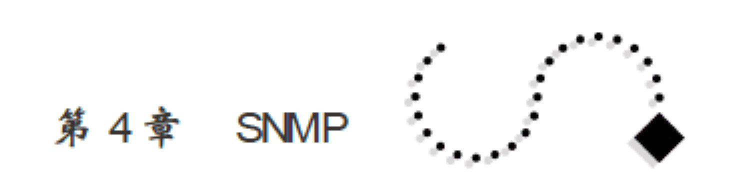
表 4-2　构造类型说明

类型标识符	说　明
SEQUENCE	一个或多个基本类型的有序集合
SEQUENCE OF	0 个或多个基本类型有序集合的数组
SET	一个或多个基本类型的无序集合
SET OF	0 个或多个基本类型无序集合的数组

2. ASN.1 转换语法

ASN.1 只能在设计时写在纸上，为了能够在实际的应用中也使用 ASN.1，设计者又定义了 ASN.1 的转换语法，它定义了 ASN.1 类型的值如何转换为适合传输的字节序列。

ASN.1 转换语法是使用基本编码规则(Basic Encoding Rules，BER)进行二进制代码编写的。BER 的编写规则是：每一个传输的值，不论是固有的(原语)，还是用户自定义(构造)的，最多由三个字段组成。



- 标识符：包括类型和标记。
- 数据字段的长度，以字节为单位。
- 数据字段。

标识符位于第一个字段，它标识了后面的项，其本身有三个子字段，如图 4-2 所示。

Tag(6、7位)	Type(5位)	Number(4、3、2、1、0位)

图 4-2 标识符字段

标识符最高两位编码(Tag)标识后面数据的作用，它共有 4 种选项，如表 4-3 所示为取值及其含义。

表 4-3 标识符最高两位的取值及其含义

取值(二进制表示)	含　义
00	表示通用的(Universal)
01	表示应用程序的(Application)
10	表示上下文相关的(Context Specific)
11	表示私有的(Private)

标识符的下一位(Type)是表示类型的，取 0 时表示是原语类型(固有的)，取 1 时表示是构造类型(用户自定义的，由多个原语类型组成的“结构”体)。

标识符低 5 位(Number)是标识后面数据的数据类型的，类型表示及其标识代码如表 4-4 所示。类型也可自定，如果类型在 0～30 的范围内，则直接使用即可，但当类型代码超过 30 时，Number(低 5 位)被置为 11111(二进制全 1)，然后在后面增加一到多个字节表示，这些字节的低 7 位用来表示数据，高 1 位表示是否是结束，当高 1 位为 1 时表示是最后一个字节，其余的高 1 位均为 0。

表 4-4 数据类型及其标识代码

数据类型标识符	代码	数据类型标识符	代码
INTEGER	2	OBJECT IDENTIFIER	6
BIT STRING	3	SEQUENCE and SEQUENCE OF	16
OCTET STRING	4	SET and SET OF	17
NULL	5		

例如，私有的复合结构，类型代码为 50 的 BER 编码的二进制形式是 11111111 10110010；再例如，通用的原语结构，标识为整型的 BER 编码的二进制形式是 00000010。

数据字段的长度位于标识符字段后，但是因为标识符字段是不定长的，所以数据字段的长度项具体位于第几个字节，还要具体问题具体分析。

数据字段的长度项指出后面要用多少个字节来存储数据(注意：长度不包括这个字段本身和标识符字段)。

当数据长度小于128时，用一个字节来表示这个字段，其中最高位记为0，其余低7位用来表示长度；当长度的值大于128时，第一个字节用来说明用几个字节来表示长度，其中最高位记为1，其余低7位用来表示长度值用了几个字节。

例如，要表示的数据长度为15，则BER编码的二进制形式是00001111；再例如，要表示的数据长度为1000，则BER编码的二进制形式是10000010 00000011 11101000，其中第一字节的最高位是1，并且低7位的值是2，表示后面还有两个字节来表示数据长度，后两个字节表示实际的数据长度值1000。

数据字段项是实际数据的存储位置，它的编码依赖当前数据的类型。

如果是INTEGER类型，则以二进制的补码方式编码，小于128的正整数需要用1个字节表示，小于32 768的正整数需要用2个字节表示，以此类推。

如果是BIT STRING类型，则编码内容不变，长度域表示需要用到的字节个数，并在实际的位串之前加一个字节表示位串最后一个字节不用的位数。例如，位串010011111被编码为00000111 01001111 10000000，其中第一字节不是实际数据，它表示最后一个字节有几个位不用，本例中的值是7，也即表示最后一个字节中的最高一位有效，其余均无效；第二个字节中存储的是位串前8位的值，第三个字节的最高位中存放了位串的剩余一位，其余无效位均为0。

如果是OCTET STRING类型，则编码内容不变。

如果是NULL类型，则长度域为0，不传任何数据。

如果是OBJECT IDENTIFIER类型，则按MIB树的编码整数序列编码，每一项均按照整数编码，例如Internet是{1,3,6,1}，但是，第一个数值总是0,1或2，第二个数值总是小于40，所以前两个数可用一个字节编码，因此Internet编码后的值是{43,6,1}。

BER的编码规则非常复杂，如果没有实际的数据，就无法判断其会占用多少字节。下面列举一些例子加以说明。

INTEGER类型的50的BER二进制编码是00000010 00000001 00110010，其中第一个字节是标识符，代表INTEGER型，第二个字节是长度，代表数值项占有一个字节。

BIT STRING类型的1110的BER二进制编码是00000011 00000010 00000100 11100000，其中第一个字节是标识符，代表BIT STRING类型，第二个字节是长度，代表后面的数值占有两个字节，第三个字节表示位串的最后一个字节的后几位无效。

OCTET STRING类型的ab的BER二进制编码是00000100 00000010 01100001 01100010，其中第一个字节是标识符，代表OCTET STRING类型，第二个字节是长度，代表实际数据占用两个字节，第三字节是a的ASCII码值，第四个字节是b的ASCII码值。

NULL类型的BER二进制编码是0000101 00000000，其中第一个字节表示标识符，代表NULL类型，长度为0，值域项没有。

OBJECT IDENTIFIER类型的“1.3.6.1”的BER二进制编码是00000110 00000011 00101000 00000110 00000001，其中第一个字节表示标识符，代表OBJECT IDENTIFIER类型，长度为3，代表实际数据共占有三个字节（“1.3”两个值共占一个字节），第三个字节表示“1.3”，第四个字节表示“6”，第五个字节表示“1”。



3. SMI

在实际的设备中所有的管理信息和对象都存放在库中(MIB),为了方便人们的记忆和管理,设计者使用了一个有层次的树状结构来表示这些管理对象。SMI 对于 MIB 来说就相当于模式对于数据库。SMI 定义了每一个对象"看上去像什么"。图 4-3 显示了 SMI 定义的 MIB 树的顶部。

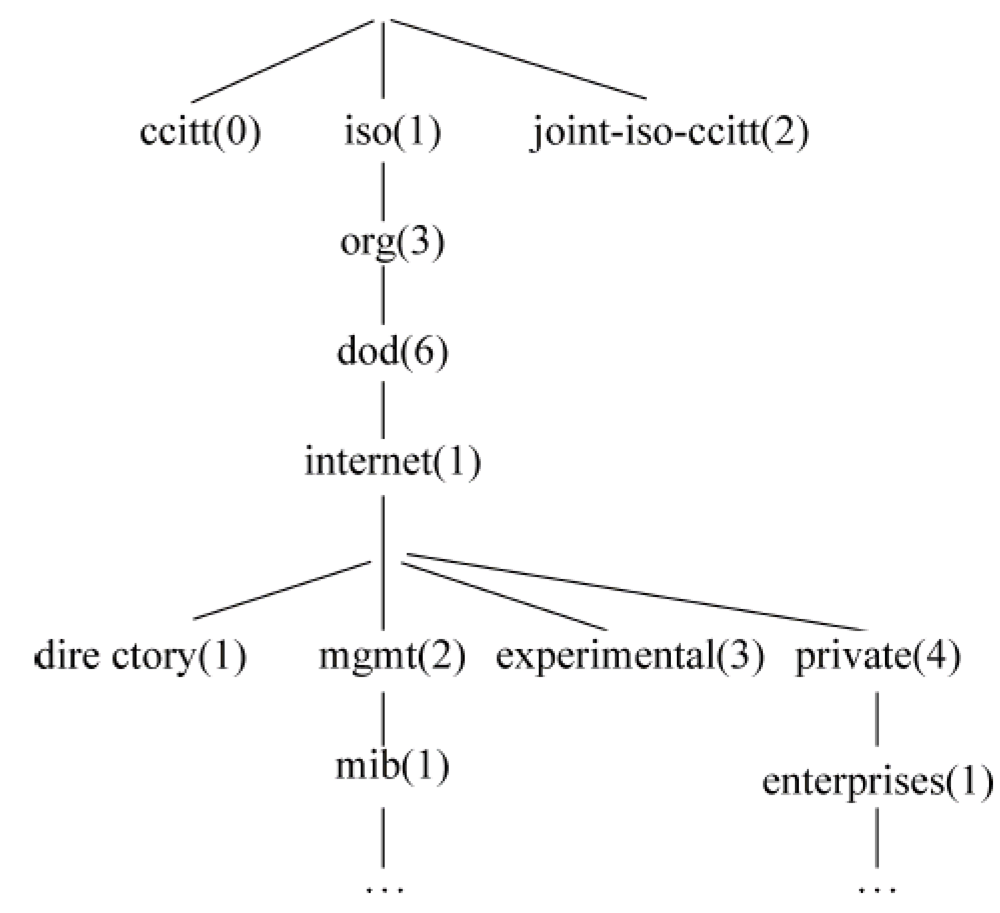


图 4-3 RFC1155(SMI)定义的 MIB 树的顶部图

在这个树状结构中,internet 对象可以由以下代码标识:{iso(1) org(3) dod(6) internet(1)}或者简记为{1. 3. 6. 1}。

这种标识方法叫作对象标识符(Object Identifier,OID),用于标识一个管理对象,以及在 MIB 中如何访问该对象。

每一个 OID 在整个 MIB 树中都是唯一的,就如同实际生活中每一个中华人民共和国的公民都会有一个与自己相对应的身份证号,这个号码由省(或直辖市等)号、市号、出生年月、编号以及校验码组成,这种按层次的组成方法可以保证每一个人都有一个唯一的号码,而且通过这种方法可以非常容易地记忆和查询。

SMI 不定义 MIB 对象,但其规定了定义管理对象的格式。一个对象定义通常包括 5 个域。

- OBJECT:是一个字符串名,它叫 OBJECT DESCRIPTOR,它指定对象类型,这个类型和 OBJECT IDENTIFIER 相对应。
- SYNTAX:对象类型的抽象语法。它必须可以解析到 ASN. 1 类型 OBJECT SYNTAX 的一个实例上。
- DEFINITION:对象类型语义的文本描述。实现中必须保证对象的实例满足这个定义,因为这个 MIB 是用于多厂商环境中的,要照顾到它们的情况。对象在不同的机器上有相同的意义是很重要的,这要靠文本约束。
- ACCESS:取只读、读写、只写或不能访问这 4 个值。
- STATUS:强制(mandatory)、可选(optional)或过时的(obsolete)。

其中,语法是根据对象类型定义对象结构的,定义时使用 ASN. 1,但 ASN. 1 中的一些通用化需要加以限制。SMI 中使用三种语法:原始类型、构造类型和自定义类型。

原始类型和构造类型在 4. 1 节中已经讲解过了。原始类型包括 INTEGER、OCTET STRING、OBJECT IDENTIFIER 和 NULL 等。构造类型使用 SEQUENCE 或 SEQUENCE OF 建立行或表。

SMI 允许在一个新应用产品的范围内由用户自定义类型,但这些类型必须能够分解为基本类型、行、表或其他自定义类型。SMI 中定义了用于 SNMP 的一些自定义类型,其类型值和说明如表 4-5 所示。

表 4-5 SMI 自定义类型值及其说明

SMI 自定义类型值	说 明
NetworkAddress	此类型代表多个可能的协议簇中的一个地址格式，当前只有 Internet 协议簇
IpAddress	此类型代表 32 位的 IP 地址，它表示为长度为 4 的字符串。在 ASN.1 类型使用 BER 规则进行编码时，只能使用原始编码形式
Counter	这种定义的类型代表一个非负整数，它只能增加，直到最大值。当达到最大值后，它会返回 0 重新开始。RFC1155 指定它的最大值为 $2^{32}-1$，也就是 4 294 967 295。它也称为循环计数器，是定义对象时常见的类型之一。此类型典型的应用是对接收或发送的数据包和字节的数目计数
Gauge	此类型代表一个非负整数，它可以增加或减少，但在最大值时停止。RFC1155 指定它的值为 4 294 967 295
TimeTicks	此类型为非负整数，用于记录从一个时间点起经过了多少个百分之一秒的时间。此类型是和计时器相关的，是两个时间点的差值，所以定义时需要在描述里告诉用户这两个时间参考点
Opaque	此类型支持对 ASN.1 语法进行扩充。此类型只要求接收方能够对数据进行解密，并没有要求接收方一定要理解其内容
DisplayString	可打印的字符串，使用可读的字符，是一种方便阅读的类型。定义为 DisplayString∷= OCTET STRING
PhysAddress	存放接口的 MAC 地址。定义为 PhysAddress∷= OCTET STRING

如图 4-4 所示为两个 SMI 的例子。第一个例子是叫作 lostPackets 变量，它用于路由器或其他处理分组的设备。第二个例子是叫作 ipAddrTable 的变量，它用于描述地址表，其类型是一个构造类型，∷=符号后的值指明它在 MIB 树上的位置。

4.2.2 MIB-2 功能组

在 RFC1156 文档中定义了 SNMP 第一个版本的管理信息库（MIB-1），随后又在 RFC1213 文档中定义了第二个版本的管理信息库（MIB-2）。MIB-2 是对 MIB-1 进行的扩展和修改，现在的 SNMP 都是以 MIB-2 为基准的。

1. MIB-2 功能组

MIB-2 由 9 个功能组组成。

- system 组：提供运行代理的设备或系统的全部信息。
- interfaces 组：包含关于系统中网络接口的信息。
- at 组：IP 地址到数据链路地址的地址转换表，但是这个组随着 RFC1213 的引退而逐渐被放弃了，其内容也被移到了其他的文档（组）中。
- ip 组：包含关于设备的 IP 地址信息。
- icmp 组：包含关于设备的 Internet 控制消息协议的信息。
- tcp 组：包含关于设备的传输控制协议的信息。
- udp 组：包含关于设备的用户数据报协议的信息。
- egp 组：包含关于设备的外部网关协议的信息，随着 SNMP 的发展，这个组现在也已经不再使用了。

```
lostPackets OBJECT-TYPE
    SYNTAX Counter          --use a 32-bit counter
    ACCESS read-only        --the management station may not change it
    STATUS current          --this variable is not obsolete (yet)
    DESCRIPTION
        "The number of packets lost since the last boot."
    : := {experimental 20}

ipAddrTable OBJECT-TYPE
    SYNTAX
        ipAddrEntry ::= SEQUENCE{
                ipAdEntAddr
                    ipAddress,
                ipAdEntIfIndex
                    INTEGER,
                ipAdEntNetMask
                    ipAddress,
                ipAdEntBcastAddr
                    INTEGER,
                ipAdEntReasmMaxSize
                    INTEGER (0..65535)
                }
    ACCESS not-accessible
    STATUS mandatory
    DESCRIPTION
        "The table of addressing kinformation relevant to this entity's IP address."
    : := {ip 20}
```

图 4-4　SMI 定义示例

- snmp 组：包含关于设备的简单网络管理协议的信息。

2. MIB-2 功能组的常用对象

（1）system 组

system 组提供有关被管系统的总体信息。表 4-6 列出了该组中各个对象的名称、句法、访问权限和对象描述。

表 4-6　system 组中的对象

Object	Syntax	Access	Description
sysDescr	DisplayString（SIZE(0…255)）	RO	对实体的描述，如硬件、操作系统等
sysObjectID	OBJECT IDENTIFIER	RO	实体中包含的网络管理子系统的厂商标识
sysUpTime	TimeTicks	RO	系统的网络管理部分本次启动以来的时间
sysContect	DisplayString（SIZE(0…255)）	RW	该被管节点负责人的标识和联系信息
sysName	DisplayString（SIZE(0…255)）	RW	该被管节点被赋予的名称

续表

Object	Syntax	Access	Description
sysLocation	DisplayString (SIZE(0…255))	RW	该节点的物理地点
sysService	INERGER(0…127)	RO	指出该节点所提供的服务的集合，7个比特对应7层服务

（2）interfaces 组

interfaces 组包含实体物理接口的一般信息，包括配置信息和各接口中所发生的事件的统计信息。表 4-7 列出了该组中各个对象的名称、句法、访问权限和对象描述。

表 4-7　interfaces 组中的对象

Object	Syntax	Access	Description
ifNumber	INTEGER	RO	网络接口的数目
ifTable	SEQUENCE OF ifEntry	NA	接口条目清单
ifEntry	SEQUENCE	NA	包含子网及其以下层对象的接口条目
ifIndex	INTEGER	RO	对应各个接口的唯一值
ifDescr	DisplayString (SIZE(0…255))	RO	有关接口的信息，包括厂商、产品名称、硬件接口版本
ifType	INTEGER	RO	接口类型，根据物理或链路层协议区分
ifMtu	INERGER	RO	接口可接收或发送的最大协议数据单元的尺寸
ifSpeed	Gauge	RO	接口当前数据速率的估计值
ifPhysAddress	PhysAddress	RO	网络层之下协议层的接口地址
ifAdminStatus	INTEGER	RW	期望的接口状态（up(1)，down(2)，testing(3)）
ifOperStatus	INTEGER	RO	当前的操作接口状态（up(1)，down(2)，testing(3)）
ifLastChange	TimeTicks	RO	接口进入当前操作状态的时间
ifInOctets	Counter	RO	接口收到的 8 元组的总数
ifInUcastPkts	Counter	RO	递交到高层协议的子网单播的分组数
ifInNUcastPkts	Counter	RO	递交到高层协议的非单播的分组数
ifInDiscards	Counter	RO	被丢弃的进站分组数
ifInErrors	Counter	RO	有错的进站分组数
ifInUnkownProtos	Counter	RO	由于协议未知而被丢弃的分组数
ifOutOctets	Counter	RO	接口发送的 8 元组的总数
ifOutUcastPkts	Counter	RO	发送到子网单播地址的分组总数
ifOutNUcastPkts	Counter	RO	发送到非子网单播地址的分组总数

续表

Object	Syntax	Access	Description
ifOutDiscards	Counter	RO	被丢弃的出站分组数
ifOutErrors	Counter	RO	不能被发送的有错的分组数
ifOutQLen	Gauge	RO	输出分组队列长度
ifSpecific	OBJECT IDENTIFIER	RO	参考 MIB 对实现接口的媒体的定义

(3) address translation 组

address translation 组由一个表构成,表中的每一行对应系统中的一个物理接口,提供网络地址向物理地址的映射。一般情况下,网络地址是指系统在该接口上的 IP 地址,而物理地址决定于实际采用的子网情况。例如,如果接口对应的是 LAN,则物理地址是接口的 MAC 地址,如果对应 X. 25 分组交换网,则物理地址可能是一个 X. 121 地址。表 4-8 列出了该组中各个对象的名称、句法、访问权限和对象描述。

表 4-8 address translation 组中的对象

Object	Syntax	Access	Description
atTable	SEQUENCE OF AtEntry	NA	包含网络地址对物理地址的映射
atEntry	SEQUENCE	NA	包含一个网络地址、物理地址对
atIfIndex	INTEGER	RW	表格条目的索引
atPhysAddress	PhysAddress	RW	依赖媒体的物理地址
atNetAddress	NetworkAddress	RW	对应物理地址的网络地址

实际上,address translation 组包含在 MIB-2 中只是为了与 MIB-1 兼容,MIB-2 的地址转换信息在各个网络协议组中提供。

(4) ip 组

ip 组包含有关节点上 IP 实现和操作的信息,如有关 IP 层流量的一些计数器。ip 组中包含三个表,ipAddrTable、ipRouteTable 和 ipNetToMediaTable。

ipAddrTable 包含分配给该实体的 IP 地址的信息,每个地址被唯一地分配给一个物理地址。

ipRouteTable 包含用于互联网路由选择的信息。该路由表中的信息是从一些协议的路由表中抽取而来的。实体当前所知的每条路由都有一个条目,表格由 ipRouteDest 索引。ipRouteTable 中的信息可用于配置的监测,并且由于表中的对象是 read-write 的,因此也可被用于路由控制。

ipNetToMediaTable 是一个提供 IP 地址和物理地址之间对应关系的地址转换表。除了增加一个指示映射类型的对象 ipNetToMediaType 之外,表中所包含的信息与 address translation 组相同。

此外,ip 组中还包含一些用于性能和故障监测的标量对象。

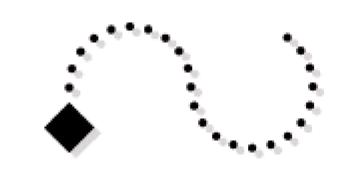


表4-9列出了该组中各个对象的名称、句法、访问权限和对象描述。

表4-9　ip组中的对象

Object	Syntax	Access	Description
ipForwarding	INTEGER	RW	是否作为IP网关(1/0)
ipDefaultTTL	INTEGER	RW	插入该实体生成的数据报的IP头Time-To-Live字段中的默认值
ipInReceives	Counter	RO	接口收到的输入数据报的总数
ipInHdrErrors	Counter	RO	由于IP头错被丢弃的输入数据报总数
ipInAddrErrors	Counter	RO	由于IP地址错被丢弃的输入数据报总数
ipForwDatagrams	Counter	RO	转发的输入数据报数
ipInUnknownProtos	Counter	RO	由于协议未知而被丢弃的输入数据报数
ipInDiscards	Counter	RO	无适当理由而被丢弃的输入数据报数
ipInDelivers	Counter	RO	成功地递交给IP用户协议的输入数据报数
ipOutRequests	Counter	RO	本地IP用户协议要求传输的IP数据报总数
ipOutNoRoutes	Counter	RO	由于未找到路由而被丢弃的IP数据报数
ipReasmTimeOut	INTEGER	RO	重组接收到的碎片可等待的最大秒数
ipReasmReqds	Counter	RO	接收到的需要重组的IP碎片数
ipReasmOKs	Counter	RO	成功重组的IP数据报数
ipRaesmFails	Counter	RO	由IP重组算法检测到的重组失败的数目
ipFragsOk	Counter	RO	成功拆分的IP数据报数
ipFragsFails	Counter	RO	不能成功拆分而被丢弃的IP数据报数
ipFragsCreates	Counter	RO	本实体产生的IP数据报碎片数
ipAddrTable	SEQUENCE OF ipAddrEntry	NA	本实体的IP地址信息(表内对象略)
ipRouteTable	SEQUENCE OF ipRouteEntry	NA	IP路由表(表内对象略)
ipNetToMediaTable	SEQUENCE OF ipNetToMedis Entry	NA	用于将IP映射到物理地址的地址转换表(表内对象略)
IpRouting Discards	Counter	RO	被丢弃的路由选择条目

(5) icmp组

ICMP(Internet Control Message Protocol)是TCP/IP协议簇中的一部分，所有实现IP的系统都提供ICMP。ICMP提供从路由器或其他主机向主机传递消息的手段，它的基本作用是反馈通信环境中存在的问题，例如：数据报不能到达目的地，路由器没有缓冲区容量来转发数据报。

icmp组包含有关一个节点的ICMP实现和操作的信息，具体地讲，icmp组由节点接

收和发送的各种 ICMP 消息的计数器构成。表 4-10 列出了该组中各个对象的名称、句法、访问权限和对象描述。

表 4-10 icmp 组中的对象

Object	Syntax	Access	Description
icmpInMsgs	Counter	RO	收到的 ICMP 消息的总数
icmpInErrors	Counter	RO	收到的有错的 ICMP 的消息数
icmpInDestUnreachs	Counter	RO	收到的目的地不可到达的消息数
icmpInTimeExcds	Counter	RO	收到的超时的消息数
icmpInParmProbs	Counter	RO	收到的有参数问题的消息数
icmpInSrcQuenchs	Counter	RO	收到的源有问题的消息数
icmpInRedirects	Counter	RO	收到的重定向的消息数
icmpInEchos	Counter	RO	收到的要求 echo 的消息数
icmpInEchoReps	Counter	RO	收到的应答 echo 的消息数
icmpInTimestamps	Counter	RO	收到的要求 Timestamp 的消息数
icmpInTimestampReps	Counter	RO	收到的应答 Timestamp 的消息数
icmpInAddrMasks	Counter	RO	收到的要求 Address Mask 的消息数
icmpInAddrMaskReps	Counter	RO	收到的应答 Address Mask 的消息数
icmpOutMsgs	Counter	RO	发出的 ICMP 消息的总数
icmpOutErrors	Counter	RO	发出的有错的 ICMP 的消息数
icmpOutDestUnreachs	Counter	RO	发出的目的地不可到达的消息数
icmpOutTimeExcds	Counter	RO	发出的超时的消息数
icmpOutParmProbs	Counter	RO	发出的有参数问题的消息数
icmpOutSrcQuenchs	Counter	RO	发出的源有问题的消息数
icmpOutRedirects	Counter	RO	发出的重定向的消息数
icmpOutEchos	Counter	RO	发出的要求 echo 的消息数
icmpOutEchoReps	Counter	RO	发出的应答 echo 的消息数
icmpOutTimestamps	Counter	RO	发出的要求 Timestamp 的消息数
icmpOutTimestampReps	Counter	RO	发出的应答 Timestamp 的消息数
icmpOutAddrMasks	Counter	RO	发出的要求 Address Mask 的消息数
icmpOutAddrMaskReps	Counter	RO	发出的应答 Address Mask 的消息数

(6) tcp 组

tcp 组包含有关一个节点的 TCP 实现和操作的信息，表 4-11 列出了该组中各个对象的名称、句法、访问权限和对象描述。

表 4-11　tcp 组中的对象

Object	Syntax	Access	Description
tcpRtoAlgorithm	INTEGER	RO	重传时间
tcpRtoMin	INTEGER	RO	重传时间的最小值
tcpRtoMax	INTEGER	RO	重传时间的最大值
tcpMaxConn	INTEGER	RO	实体支持的 TCP 连接数的上限
tcpActiveOpens	Counter	RO	实体已经支持的主动打开的数量
tcpPassiveOpens	Counter	RO	实体已经支持的被动打开的数量
tcpAttemptFails	Counter	RO	已经发生的试连失败的次数
tcpEstabResets	Counter	RO	已经发生的复位的次数
tcpCurrEstab	Gauge	RO	当前状态为 established 的 TCP 连接数
tcpInSegs	Counter	RO	收到的 segments 总数
tcpOutSegs	Counter	RO	发出的 segments 总数
tcpRetranSegs	Counter	RO	重传的 segments 总数
tcpConnTable	SEQUENCE OF tcpConnTntry	NA	包含 TCP 各个连接的信息
tcpInErrors	Counter	RO	收到的有错的 segments 的总数
tcpOutRsts	Counter	RO	发出的含有 RST 标识的 segments 数

（7）udp 组

udp 组包含有关一个节点的 UDP 实现和操作的信息。除了有关发送和接收的数据报的信息之外，这个组中还包含一个 udpTable 表，该表中包含 UDP 端点的管理信息。所谓 UDP 端点是指正在支持本地应用接收数据报的 UDP 进程。udpTable 表中包含每个 UDP 端点用户的 IP 地址和 UDP 端口。表 4-12 列出了该组中各个对象的名称、句法、访问权限和对象描述。

表 4-12　udp 组中的对象

Object	Syntax	Access	Description
udpInDatagrams	Counter	RO	递交该 UDP 用户的数据报的总数
udpNoPorts	Counter	RO	收到的目的端口上没有应用的数据报总数
udpInErrors	Counter	RO	收到的无法递交的数据报数
udpOutDatagrams	Counter	RO	该实体发出的 UDP 数据报总数
udpTable	SEQUENCE OF udpEntry	NA	包含 UDP 的用户信息
udpTable	SEQUENCE	NA	某个当前 UDP 用户的信息
udpLocalAddress	ipAddress	RO	UDP 用户的本地 IP 地址
udpLocalPort	INTEGER	RO	UDP 用户的本地端口号

(8) egp 组

egp 组包含有关一个节点的 EGP(External Gateway Protocol)实现和操作的信息。除了有关发送和接收的 EGP 消息的信息之外,这个组中还包含一个 egpNeighTable 表,该表中包含有关相邻网关的信息。表 4-13 列出了该组中各个对象的名称、句法、访问权限和对象描述。

表 4-13 egp 组中的对象

Object	Syntax	Access	Description
egpInMsgs	Counter	RO	收到的无错的 EGP 消息数
egpInErrors	Counter	RO	收到的有错的 EGP 消息数
egpOutMsgs	Counter	RO	本地产生的 EGP 消息总数
egpOutErrors	Counter	RO	由于资源限制没有发出的本地产生的 EGP 消息数
egpNeighTable	SEQUENCE OF EgpNeighEntry	NA	相邻网关的 EGP 表(表内的对象略)
egpAs	INTEGER	RO	本 EGP 实体的自治系统数

4.3 SNMP 通信模型

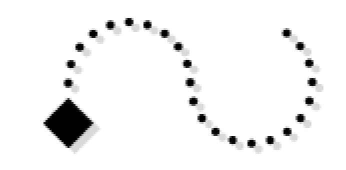
简单网络管理协议(SNMP)最初是由 Internet 工程任务组织(IETF)的研究小组为了解决 Internet 上的路由器管理问题而提出的。SNMP 被设计成与协议无关,可以在 IP、IPX、AppleTalk、OSI 以及其他用到的传输协议上使用。SNMP 包括一系列协议组和规范,它们提供了一种从网络上的设备中收集网络管理信息的方法,同时它也为设备向网络管理站报告问题提供了一种手段。

SNMP 的结构分为 SNMP 管理者和 SNMP 代理两部分。管理者从代理中收集数据有两种方法:一种是只轮询的方法;另一种是基于中断的方法。

只轮询的方法,是由管理者每间隔一段时间,向各个代理依次发送询问信息,然后由代理返回查询结果,这种方法可以使代理总是在管理者的控制之下。但这种方法的缺陷在于信息的实时性比较差。因为如果轮询间隔太小,那么将产生太多不必要的通信量。如果轮询间隔太大,并且在轮询时顺序不对,那么对于一些大的灾难性事件的通知就会太慢。

基于中断的方法是当有异常事件发生时,由代理主动向管理者发送信息,使管理者可以及时地了解网络设备的状态。但是这种方法也有一定的缺陷,当异常事件发生且要传送的信息量较大时,这种方法需要消耗大量的系统资源,从而影响了代理执行的主要功能,另外当多个代理同时发生中断时,网络将变得非常拥挤。

基于上述两种方法的优点和缺点,SNMP 把它们结合使用,形成了面向自陷的轮询方法,它是执行网络管理最为有效的方法。一般情况下,管理者通过轮询代理进行信息收集,在控制台上用数字或图形来显示这些信息,提供对网络设备工作状态和网络通信量的分析和管理功能。当代理设备处于异常状态时,代理通过 SNMP 自陷立即向网络管理者



发送通知。SNMP 定义了 get、get-next 和 set 三种基于轮询的操作，并且还定义了基于中断的 trap 操作。

4.3.1 SNMP 数据单元

SNMP 的工作原理非常简单，在管理者和代理之间实时传递信息，这些信息被称为协议数据单元(PDU)，在 SNMP 中一共定义了 4 类协议数据单元，如图 4-5 所示为这 4 种操作的示意图。

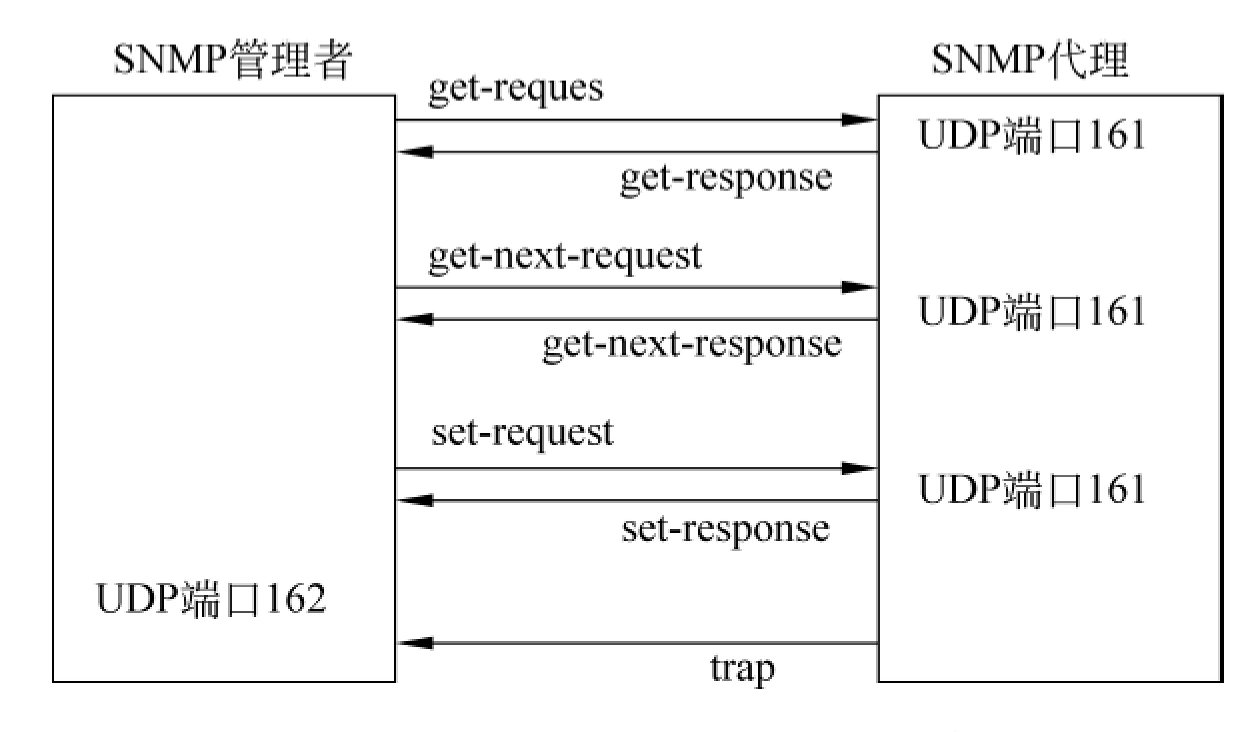


图 4-5 SNMP 4 种报文的操作示意图

SNMP 被封装在 UDP 中，前三种操作使用 UDP 的 161 端口，由代理发出的 trap 操作使用 UDP 的 162 端口。如图 4-6 所示为 SNMP 4 种操作的报文格式。

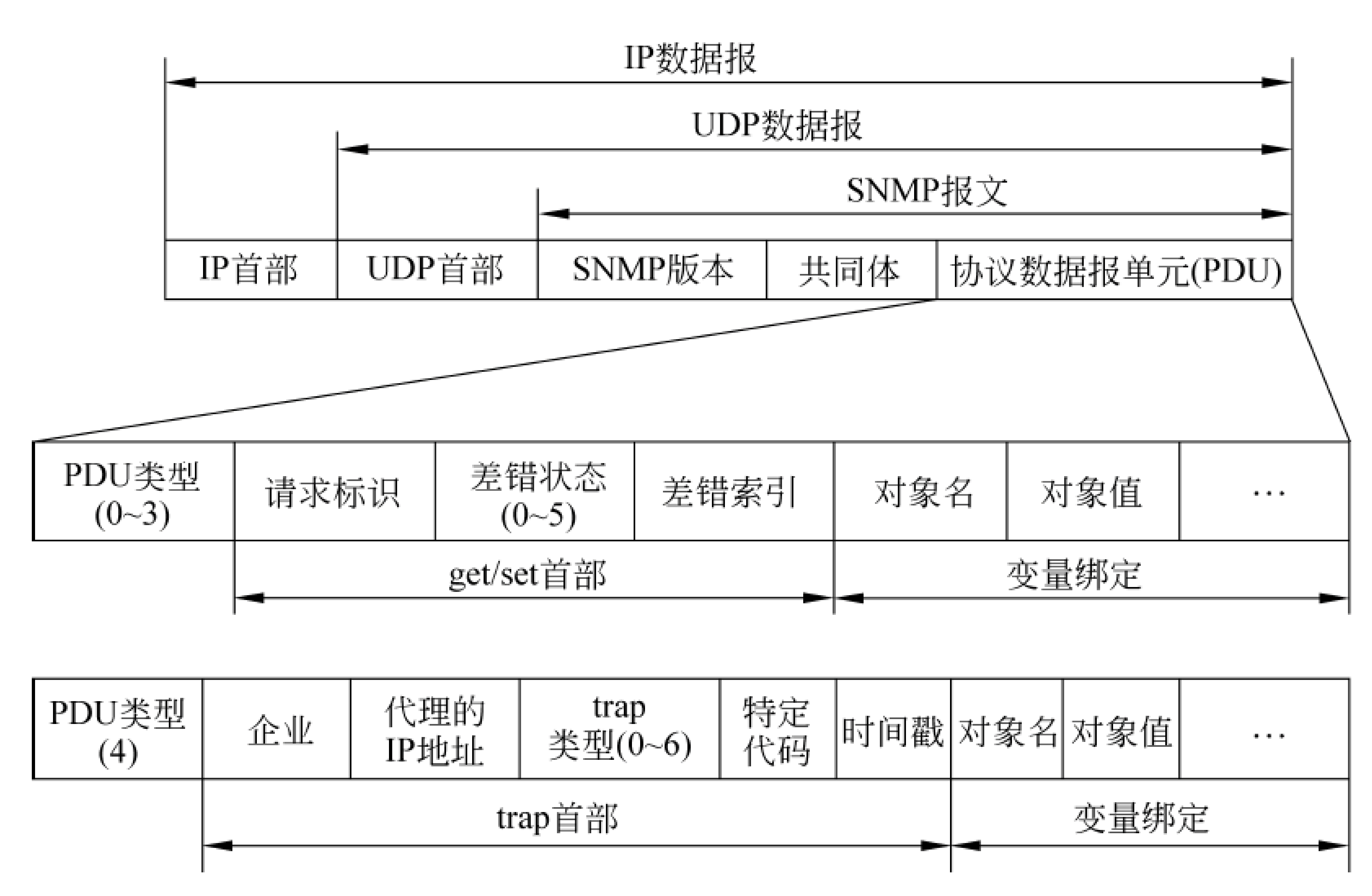
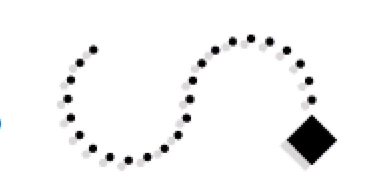


图 4-6 SNMP 报文格式

1. SNMP 版本与共同体

SNMP 的报文一般包括三个部分：SNMP 版本、共同体和协议数据单元(PDU)。

SNMP 版本用于标识管理者和代理使用的是哪个版本的 SNMP，到现在为止可以使用的 SNMP 版本共有三个，分别是：SNMP v1、SNMP v2 和 SNMP v3。在这项中存放的



版本值比实际应用的版本号小 1，如管理者或代理使用的是 SNMP v1，则这项中的值是 0。

共同体是一个字符串，作为管理者与代理之间的明文口令，常用的是 6 个字符，值是 public，当然也可以由管理员设置。协议数据单元(PDU)是 SNMP 报文的主要内容，它有两种报文类型：get/set 报文和 trap 报文。

2. get/set 报文

get/set 报文基于轮询的操作，由管理者首先向代理发出查询或设置命令，然后由代理返回操作结果。get/set 主要包括 PDU 类型、请求标识、差错状态、差错索引和变量绑定等几部分。

PDU 类型用来表示 SNMP 报文的功能，共有 5 个值可以使用，如表 4-14 所示。PDU 类型项中的值是一个特殊类型(上下文相关的构造类型)的值，只用一个字节来表示。

表 4-14 PDU 类型

PDU 类型	名　称	二进制值	十六进制值
0	get-request	10100000	0xa0
1	get-next-request	10100001	0xa1
2	get-response	10100010	0xa2
3	set-request	10100011	0xa3
4	Trap	10100100	0xa4

请求标识是由管理进程设置的一个整数值。每一个进程都有一个相应的标识，使管理进程能够识别返回的响应报文对应于哪一个请求报文，同一请求报文和响应报文使用同一个标识。

差错状态是由代理设置的一个值，用于标识返回的报文是否有错，以及出现了什么样的错误。差错状态有 6 个值可以使用，如表 4-15 所示。

表 4-15 差错状态

差错状态	名　称	描　述
0	noError	没有错误
1	tooBig	代理进程无法把响应放在一个 SNMP 消息中发送
2	noSuchName	操作一个不存在的变量
3	badValue	set 操作的值或语义有错误
4	readOnly	管理进程试图修改一个只读变量
5	genError	其他错误

差错索引也是一个由代理设置的值，它指明当有差错发生时，是在哪个变量发生的(即变量列表中的偏移)。注意并不是所有差错都有差错索引，只有发生差错 2、3 和 4 时才会有差错索引。

变量绑定是由一个或多个对象名和对象值对组成的。在 get-request 和 get-next-request 操作时，对象名由管理者设置，并把对象值设置为空(NULL)类型，代理收到后就根据对象名查询对应的对象值，如果找到，就把对象名和对象值返回给管理者。如果是 set-request 操作，则对象名和对象值均由管理者设置，代理收到后只把对应的对象名的值改为管理者设置的对象值。变量绑定中可以出现多个对象名和对象值对，即一个 SNMP 报文可以查询(get 操作)或设置(set 操作)多个对象。

3. trap 报文

trap 报文是基于中断的操作，当代理设备发生异常时，代理即向管理者发送这个报文。trap 报文主要包括 PDU 类型、企业、代理的 IP 地址、trap 类型、特定代码、时间戳和变量绑定等几部分。

PDU 类型在 trap 报文中固定为 4。

企业项是 trap 报文的网络设备的对象标识符。此对象标识符在 MIB 树上的 enterprise 节点{1.3.6.1.4.1}下面的一棵子树上。

代理的 IP 地址项表明代理设备的 IP 地址是何值。

trap 类型表明 trap 报文的类型，共有 7 种选项，如表 4-16 所示。

表 4-16 trap 类型

trap 类型	名　称	说　明
0	coldStart	代理进行了初始化
1	warmStart	代理进行了重新初始化
2	linkDown	一个接口从工作状态变为故障状态
3	Linkup	一个接口从故障状态变为工作状态
4	authenticationFailure	从 SNMP 管理进程接收到具有一个无效共同体的报文
5	egpNeighborLoss	一个 EGP 相邻路由器变为故障状态
6	enterprisespecific	在这个特定的代码字段中查找 trap 信息

注意：当使用 trap 类型 2、3、5 时，在报文后面的变量部分的第一个变量对应标识响应的接口。

特定代码项当 trap 类型为 6 时指明代理自定义的事件，否则为 0。

时间戳项指明自代理进程初始化到 trap 报告的事件发生所经历的时间，单位为 10ms。

变量绑定的内容与 get/set 报文中的变量绑定相同。

4.3.2 SNMP 的安全机制

在网络管理系统的代理设备上存放着大量的管理信息库，它们的安全直接影响到整个网络系统的安全。为了保证代理能够保护其自身以及 MIB，使 MIB 能够拒绝非法访问，需要设置一些安全机制。

在 SNMP 中，代理不但要控制自己本地的 MIB，而且必须控制多个管理者对该 MIB

的使用。这种控制包含三个方面。

- 认证服务：代理可以把对 MIB 的访问权限限制为已被授权的管理者。
- 访问策略：代理可以给不同的管理者不同的访问特权。
- 转换代理服务：一个代理可以作为其他被管理站的转换代理。这可能包括在转换代理系统中，为其他的被管理系统实现认证服务或访问策略。

1. SNMP v1 的安全机制

SNMP v1 是 SNMP 的第一个版本，其安全性上的设计非常简单，仅仅提供了有限的安全机制，即共同体的概念。

共同体的概念在 4.3.1 小节中已经提到过，它是一个明文的字符串，每一个 SNMP 共同体都是一个在 SNMP 代理和多个 SNMP 管理者之间定义的认证、访问控制和转换代理的关系。管理者发送的每一个报文中，都必须填写好对应的共同体项，当代理收到这些报文，它就比对共同体的内容，如果正确则被允许访问对应的对象，反之则被拒绝。共同体在这里起到密码的作用，SNMP v1 假设，如果发送者知道这个密码，就认为该信息通过了认证，是可靠的。

共同体不但有认证功能，还有设置访问权限的功能。一条已通过认证的信息对 MIB 有何访问权限也是通过共同体来实现的。代理为每一个共同体定义了一个 SNMP v1 共同体框架文件，该框架文件包括两部分。

- MIB 视图：MIB 中的对象的一个子集，对不同的共同体可以定义不同的视图，属于同一视图的对象可以不必同属于一个 MIB 子树。
- 访问模式：共同体可以定义一种访问模式。

2. SNMP v2 的安全机制

由于 SNMP v1 的安全机制过于简单，因此 SNMP v2 加强了安全的考虑。SNMP 具有支持分布式网络管理、扩展数据类型、可以实现大量数据的同时传输、丰富的故障处理能力、增加集合处理功能、加强数据定义语言等特点。

此外，SNMP v2 还引入了上下文的概念。上下文是一个可被 SNMP v2 实体访问的被管理对象资源的集合，分为本地上下文和远程上下文，其中本地上下文被标识为一个 MIB 视图，远程上下文被标识为一个转换代理关系。

使用了上下文的访问控制策略由以下 4 个元素组成。

- 目标：SNMP 参加者，它按主体方的请求执行管理操作。
- 主体：SNMP 参加者，它请求目标方执行管理操作。
- 资源：管理操作在其上执行的管理信息，它可表示为一个本地 MIB 视域或一个代理关系，这一项被称为一个上下文。
- 权限：对于一个特定的上下文可允许的操作，这些操作用可允许的协议数据单元定义，由目标代表主体执行。

但是，SNMP v2 并没有完全实现预期的目标，尤其是安全性能没有得到提高，如身份验证、加密、授权和访问控制、适当的远程安全配置和管理能力等都没有实现。1996 年发布的 SNMP v2C 是 SNMP v2 的修改版本，然而就在新的文件刚刚发布时就有人发现其安全方面存在重要缺陷，而且随后的改进安全设施工作又迟迟没有进展，最后决定丢掉安

全功能，把增加的其他功能作为新标准颁布，并保留了 SNMP v1 的报文封装格式和继续使用 SNMP v1 的基于明文密钥的身份验证方式。

3. SNMP v3 的安全机制

1998 年 1 月 IETF 提出了互联网建议 RFC2271～2275，正式形成了 SNMP v3。这一系列文件定义了包含 SNMP v1 和 SNMP v2 所有功能在内的体系框架以及包含验证服务和加密服务在内的全新的安全机制，同时还规定了一套专门的网络安全和访问控制规则。RFC 2271 定义的 SNMP v3 体系结构体现了模块化的设计思想，可以简单地实现功能的增加和修改，其特点主要有：

- 安全性好，具有多种安全处理模块。
- 适应性强，适用于多种操作环境，既可以管理最简单的网络，实现基本的管理功能，又能够提供强大的网络管理功能，满足复杂网络的管理需求。
- 扩充性好，可以根据需要增加模块。

SNMP v3 主要有三个模块：信息处理和控制模块、本地处理模块和用户安全模块。

（1）信息处理和控制模块

其在 RFC2272 中定义，负责信息的产生和分析，并判断信息在传输过程中是否要经过代理服务器等。

（2）本地处理模块

它的主要功能是进行访问控制，处理打包的数据和中断。访问控制是指通过设置代理的有关信息使不同管理者的管理进程在访问代理时具有不同的权限，在协议数据单元一级完成。访问控制的策略必须预先设定。SNMP v3 通过使用带有不同参数的原语来灵活确定访问控制方式。

（3）用户安全模块

SNMP v3 与其前两个版本相比，增加了三个新的安全机制：身份验证，加密和访问控制。其中，访问控制功能由本地处理模块完成，而身份验证和数据保密服务则由用户安全模块提供。身份验证是指代理或管理者接到信息时必须首先确认信息是否来自授权的管理者或代理，以及信息在传输过程中是否改变。

这个功能的实现要求管理者和代理必须共享同一密钥。管理者使用密钥计算验证码，然后将其加入信息中，而代理则使用同一密钥从接收的信息中提取出验证码，从而得到信息。加密的过程与身份验证类似，也需要管理者和代理共享同一密钥来实现信息的加密和解密。SNMP v3 使用私钥和验证密钥来实现身份验证和加密功能。

4.3.3 SNMP 的操作

SNMP 共有 4 种操作，分别是 get-request、get-next-request、set-request 和 trap，这些操作可以实现查询或设置简单对象、查询未知对象、查询或设置表对象和陷入操作等功能。

1. 查询或设置简单对象

查询简单的对象值可以用 get-request 操作，代理响应的是 get-response 报文。如果变量绑定项中含有多个对象名，则一次还可以查询多个对象的值。接收 get-request 的 SNMP 实体以请求标识相同的 get-request 响应。特别要注意的是 get-request 操作的原

子性，即如果所有请求的对象值都可以得到，则给予应答；反之，只要有一个对象的值得不到，就可能返回下列错误条件之一：

- 变量绑定项中的一个对象无法与 MIB 中的任何对象名匹配，或者要检索的对象是一个复杂类型（如子树或表等），其没有对象实例生成，那么在这些情况下，代理返回的 PDU（即 get-response）中差错状态字段置为 noSuchName，错误索引字段设置为出错的对象名在变量绑定中的偏移量，变量绑定项中不返回任何值。
- 代理设备中的响应实体可以提供所有要检索的值，但是所请求的变量太多，一个响应 PDU 装不下，这往往是由下层协议数据单元大小限制的。这时响应实体返回一个应答 PDU，其差错状态字段置为 tooBig。
- 由于其他原因（例如代理不支持等），代理中的响应实体至少不能提供一个对象的值，则返回的 PDU 中差错状态字段置为 genError，错误索引字段设置为出错的对象名在变量绑定中的偏移量，变量绑定项中不返回任何值。

设置简单的对象值可以用 set-request 操作，代理用于响应的同样也是 get-response 报文。set-request 操作同样可以一次含有多个对象名，如果所有的对象都可以修改，则修改所有请求的对象的值；如果至少有一个对象不能修改，则所有请求的对象的值均不被修改，并在差错状态字段中指明出错原因（如对象是只读的）。

2. 查询未知对象

如果不能确定对象的名称，则可以用 get-next-request 操作查询指定对象名的下一个对象实例，但是并不要求指定的对象名必须存在，或者是子树的对象标签。get-next-request 还可以遍历整个 MIB 树。

3. 查询或设置表对象

set-request 操作用于修改对象的值，它的操作与对简单对象操作类似。get-next-request 操作可以查询表对象，或是遍历整个 MIB 树。

4. 陷入操作

陷入是由代理向管理者发出的异步事件警告，它不需要应答报文。SNMP 规定了 7 种陷入条件。

- coldStart：发送实体重新初始化，代理的配置已经改变。这种情况经常是由系统失效引起的。
- warmStart：发送实体重新初始化，但代理的配置没有改变。这种情况是正常的重启动过程。
- linkDown：链路失效通知，其中变量绑定项的第一项指明对应接口表的索引对象及其值。
- linkUp：链路启动通知，其中变量绑定项的第一项指明对应接口表的索引对象及其值。
- authenticationFailure：发送实体收到一个没有通过认证的报文。
- egpNeighborLoss：相邻的外部路由器失效或关机。
- enterpriseSpecific：由设备制造商定义的陷入条件，在特殊陷入字段项中指明具体的陷入类型。

4.3.4 SNMP 通信示例

前几节介绍了 SNMP 的操作功能以及 MIB-2 功能组的组成，下面通过实例来看一看 SNMP 报文的组成以及它是如何传输的。

1. Microsoft 网络监视器

网络的底层就是数据包，只有了解这些在网络上传输的数据包，才能真正认识网络系统。现在有很多网络数据包的捕获工具，如 SnifferPro、Ethereal 等。这些工具功能强大、操作方便、界面友好，是网络管理员维护网络必不可少的工具。

虽然这些工具非常好用，但是有些工具需要花钱购买，有些工具则安装非常复杂，因此本书并没有采用这些工具，而是使用了微软公司在 Windows Server 2000（或以上）和 Windows Server 2003 版本上自带的 Microsoft 网络监视器。Microsoft 网络监视器的位置在“控制面板”的“管理工具”中，打开后如图 4-7 所示。

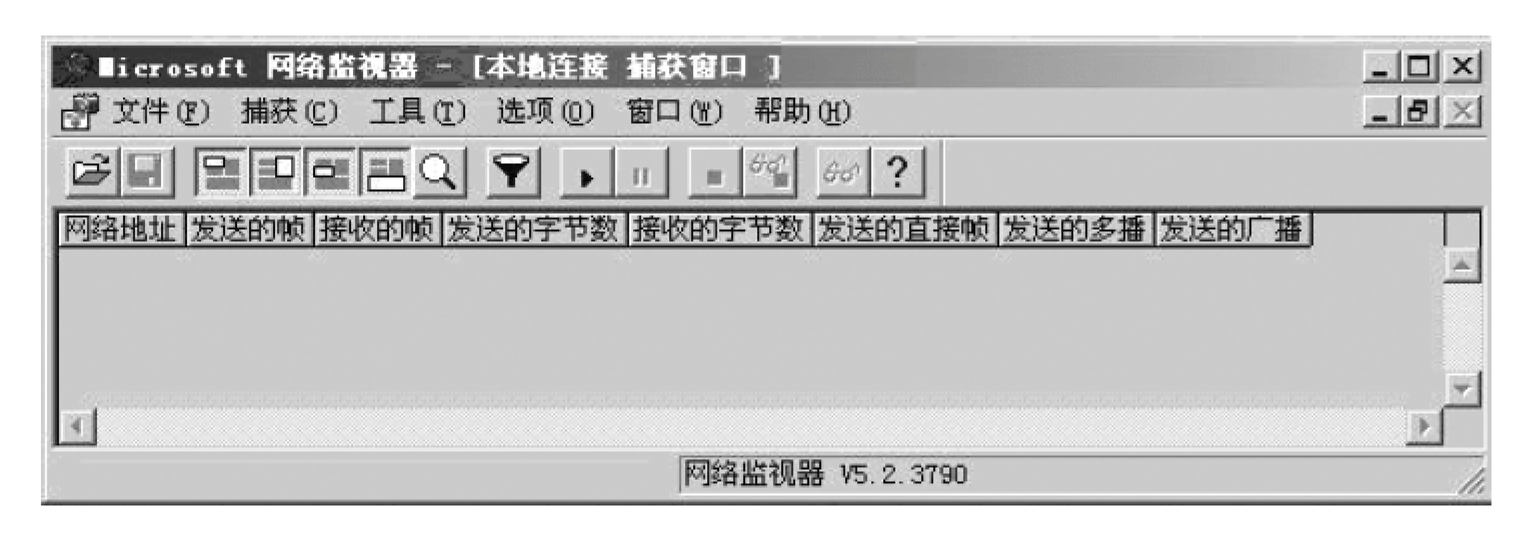


图 4-7 Microsoft 网络监视器窗口

如果是第一次使用，则在刚打开时会出现如图 4-8 所示的对话框，它的功能是让用户选择想要监视的网络接口，这里选择“本地连接”。如果在使用过程中，需要改变被监视的网络接口，则可以在“Microsoft 网络监视器”窗口中选择“捕获”→“网络”命令，也可以打开这个对话框。



图 4-8 选择一个网络对话框

选择好网络接口后就可以开始监视了，单击图 4-9 中工具栏上的“开始”按钮，这时监视器就会监听从这时起的所有网络数据包，如果需要查看数据包的详细内容，则可以单击“停止并查看”按钮，这时会出现如图 4-9 所示的窗口。如果用户对某一个数据包感兴趣，可以双击打开这个数据包，以便更详细地了解它的内容。

Microsoft 网络监视器还有很多其他功能，由于篇幅有限，这里就不一一介绍了，读者如果有兴趣，可以参看相关的参考资料。

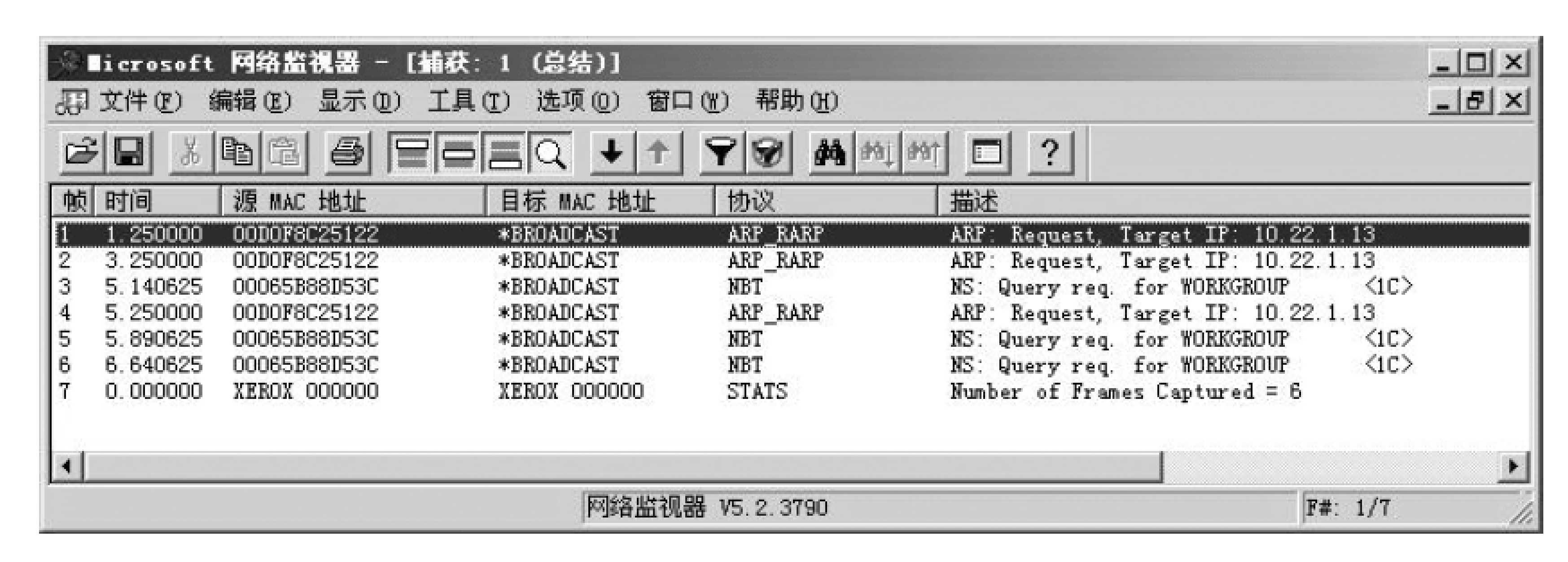


图 4-9　捕获窗口

2. Getif

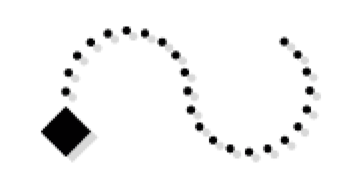
Getif 是一款免费使用的简单网络管理工具，它主要通过 SNMP 访问被管理的设备，其主界面如图 4-10 所示。

图 4-10　Getif 主界面

首先在 Host name 组合框中输入要访问的设备的 IP 地址，然后在 SNMP Parameters 选项组的 Read 和 Write 文本框中输入共同体的值(默认是 public 和 private)，最后单击 Start 按钮即可，如果被管理设备可以正常访问，则会返回相应的参数，如图 4-9 中所示，如果被管理设备不能正常访问，则在窗口最底下的状态栏中显示相应的错误信息。

Getif 工具有很丰富的功能，包括网络接口查看(Interface)、地址查看(Address)、路由表查看(Routing Table)、Arp 地址查看(Arp)、IP 地址发现(IP Discovery)等内容，由于篇幅有限，这里就不一一介绍了，读者如果有兴趣，可以参看相关的参考资料。这里主要介绍 MBrowser 选项卡，在该选项卡中可以以树状的方式查看 MIB，如图 4-11 所示。

第一个文本框中显示是 OID 标识，第二行是数字 OID 标识，中间的左侧部分是树状结构，左侧部分是这个对象的一些参数和说明，再下面是这个对象的值显示的地方。当用户在树状结构中选择了某一对象，单击 Start 按钮后，相应对象的值就会显示在这里。



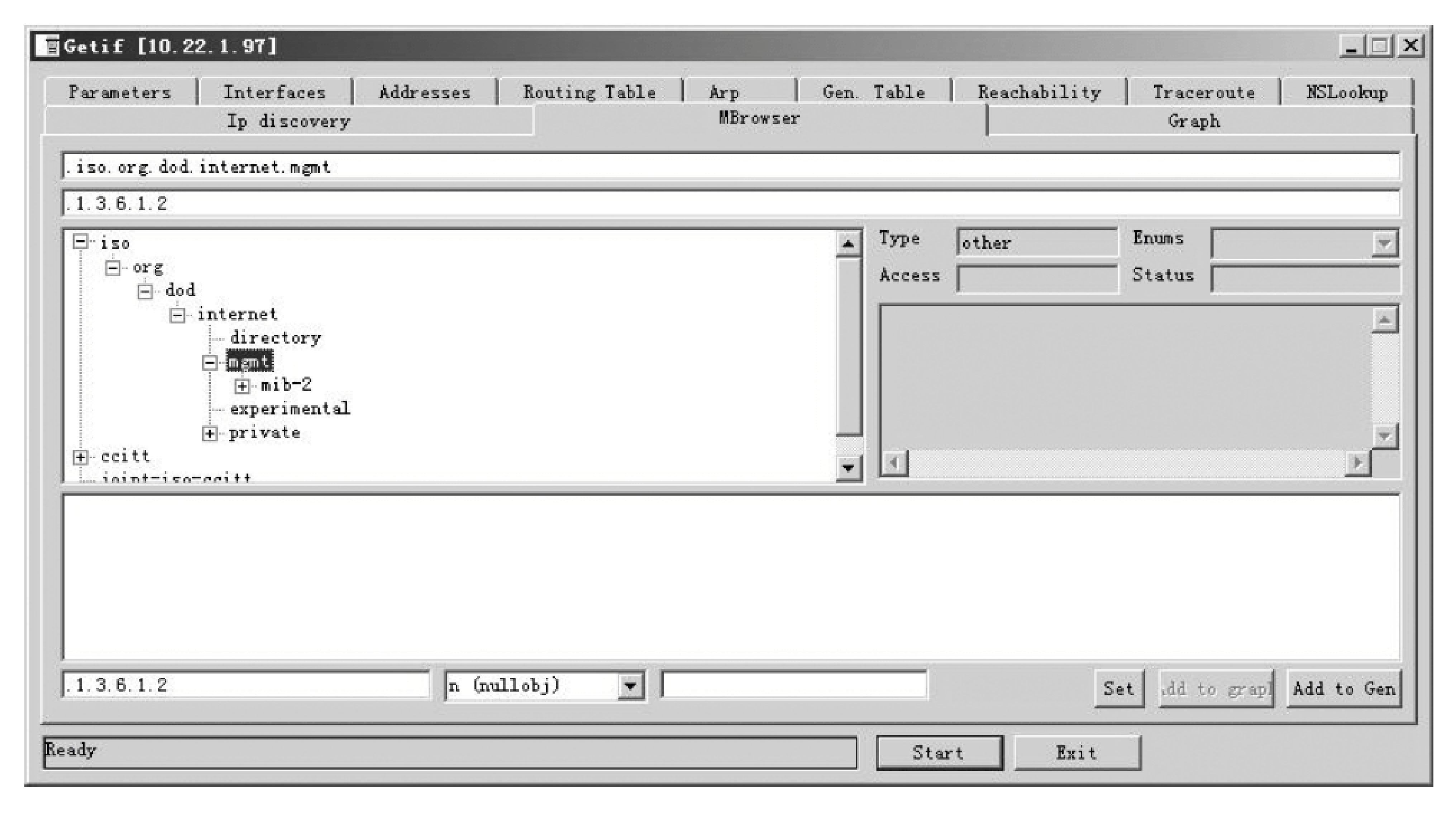


图 4-11　MBrowser 选项卡

下面演示两个例子。

第一个示例查看 OID 为.iso.org.dod.internet.mgmt.mib-2.system.sysDescr 的对象的值，首先在树状结构中选择这个对象，单击 Start 按钮，列表框中就会出现如图 4-12 所示的内容。

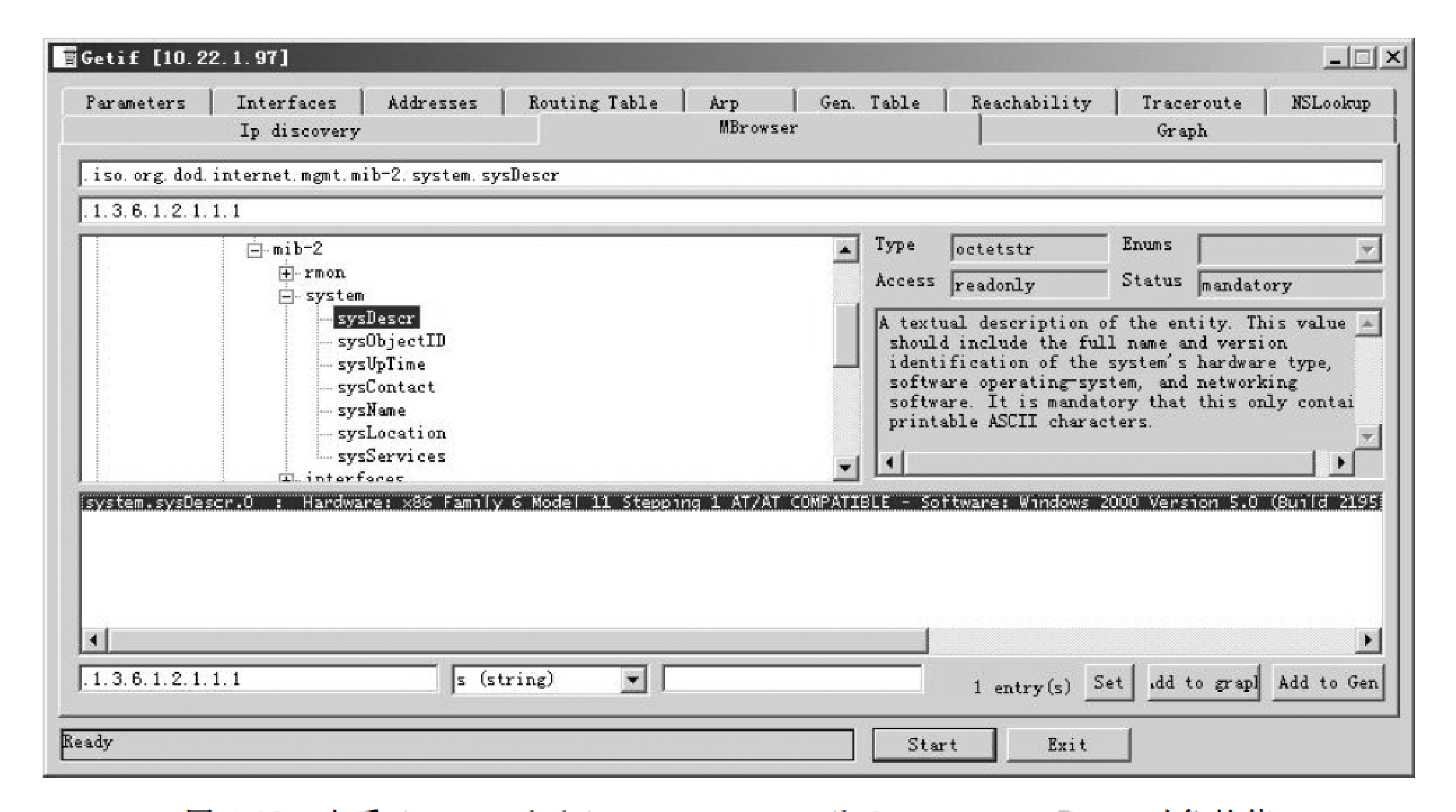


图 4-12　查看.iso.org.dod.internet.mgmt.mib-2.system.sysDescr 对象的值

第二个示例的功能是想要查看 system 组中所有成员对象的值，首先选择对象.iso.org.dod.internet.mgmt.mib-2.system，单击 Start 按钮，列表框就会出现如图 4-13 所示的内容。

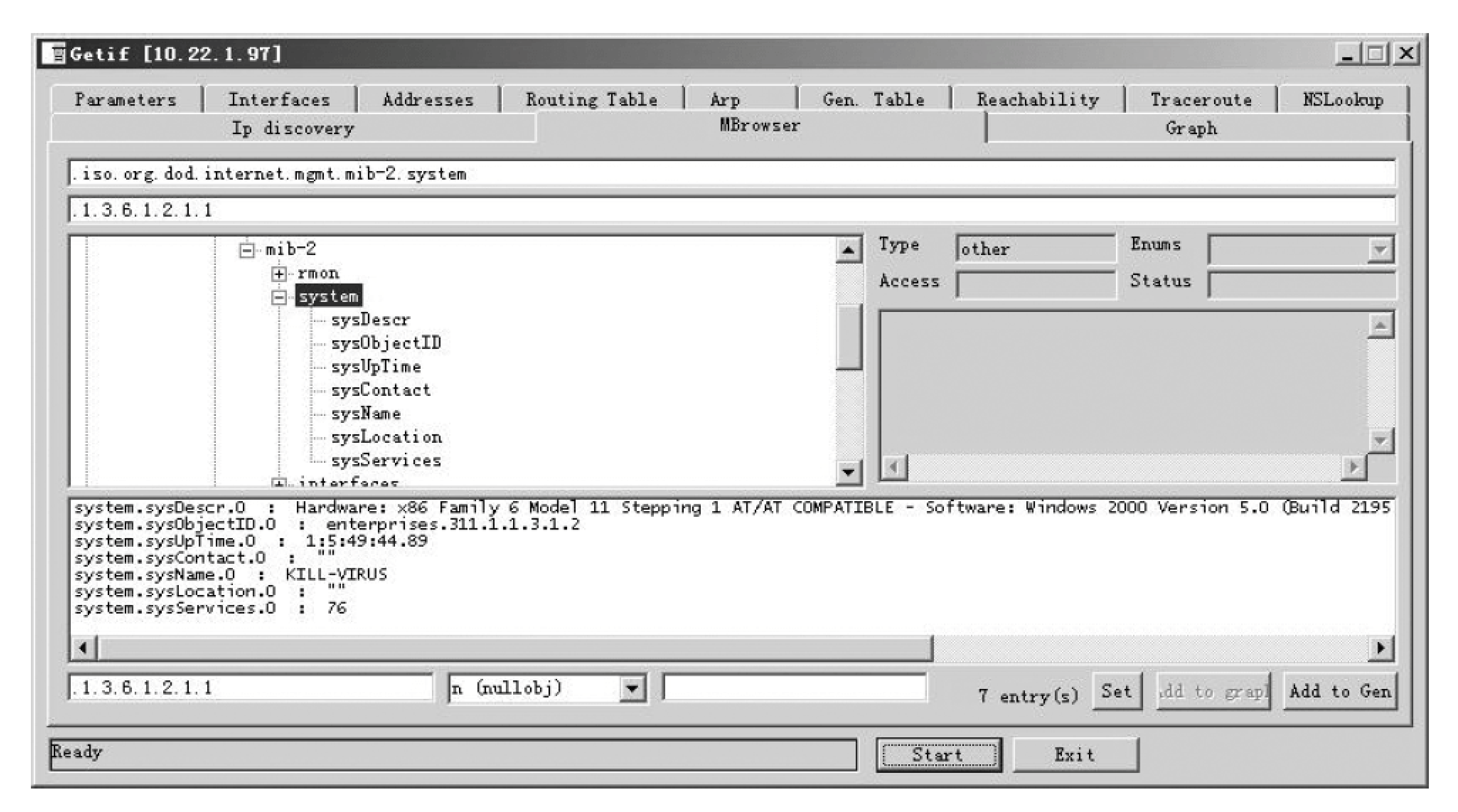


图 4-13　查看.iso.org.dod.internet.mgmt.mib-2.system 组中所有对象的值

3. 捕获和分析 SNMP 数据包

有了 Microsoft 网络监视器和 Getif，捕获和分析 SNMP 数据包就非常容易了。首先启动 Microsoft 网络监视器并开始监听，然后启动 Getif，选择相应的 OID 对象，并单击 Start 按钮，接着单击"Microsoft 网络监视器"窗口中的"停止并查看"按钮，打开如图 4-14 所示的捕获窗口，再双击相应的数据包就可以分析该数据包了。

下面举一个示例。假设要查看某一设备的 OID 为.iso.org.dod.internet.mgmt.mib-2.system.sysDescr 对象的值。按照上述步骤捕获了相应的数据包，如图 4-14 所示。

Microsoft 网络监视器 - [捕获: 1 (总结)]

文件(F) 编辑(E) 显示(D) 工具(T) 选项(O) 窗口(W) 帮助(H)

帧	时间	源 MAC 地址	目标 MAC 地址	协议	描述	其他...	其他...	其他...
1	0.014648	00D0F8C25122	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 10.22.1.13			
2	2.014648	00D0F8C25122	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 10.22.1.13			
3	2.362304	LOCAL	00065B88D53C	SNMP	SNMPv1; community = public; Get-next request; Reque...	MATAO	10.22...	IP
4	2.363281	00065B88D53C	LOCAL	SNMP	SNMPv1; community = public; Response; Request ID = ...	10.2...	MATAO	IP
5	2.363281	LOCAL	00065B88D53C	SNMP	SNMPv1; community = public; Get-next request; Reque...	MATAO	10.22...	IP
6	2.364257	00065B88D53C	LOCAL	SNMP	SNMPv1; community = public; Response; Request ID = ...	10.2...	MATAO	IP
7	4.014648	00D0F8C25122	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 10.22.1.13			
8	0.000000	XEROX 000000	XEROX 000000	STATS	Number of Frames Captured = 7			

Summary for SNMP message.　F#: 3/8　Off: 42 (x2A)　L: 48 (x30)

图 4-14　捕获数据包窗口

其中，第三个数据包是 SNMP 请求数据包，第四个数据包是 SNMP 应答数据包。首先双击第三个数据包，打开如图 4-15 所示的数据包分析窗口。

这个窗口分为三个部分，上面是捕获的数据包列表，中间是用户选中的数据包的分析情况，下面是数据包的十六进制表现形式。通过中间的数据包分析可以看到，SNMP 请求数据包分为 5 大部分(实际是 4 个)：Frame(数据包的全部数据)、Ethernet(以太网数据头部分)、IP(IP 数据头部分)、UDP(UDP 数据报头部分)和 SNMP(SNMP 数据部分)。

下面分析一下 SNMP 的数据。

- Message type：SNMP 报文类型。这个例子中 SNMP v1 对应的十六进制的值是

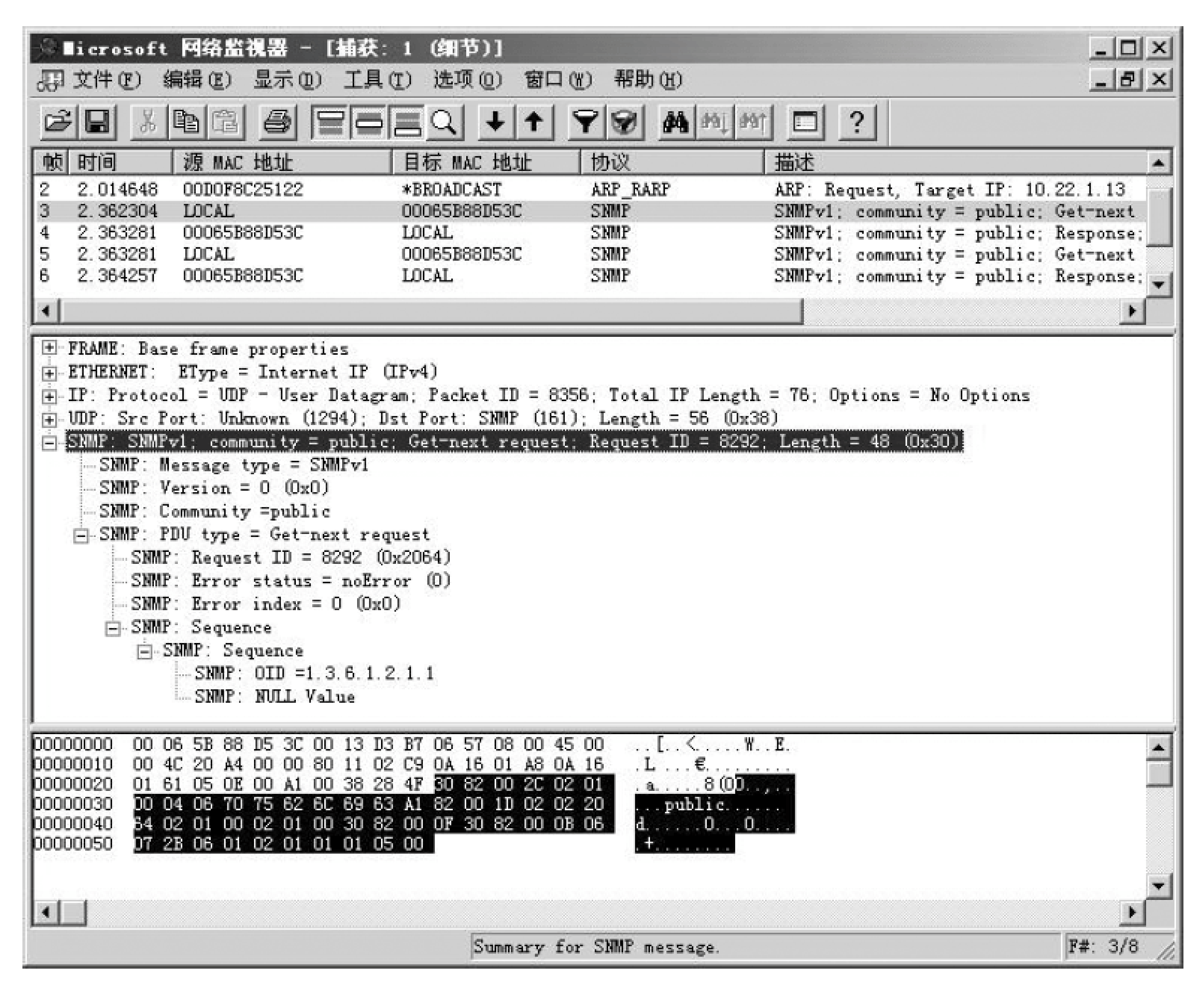
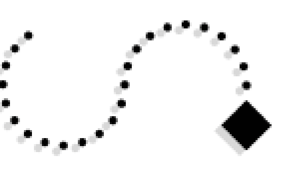


图 4-15　数据包分析窗口(1)

30，表示后面的数据是一个复合的构造类型。再后面的十六进制值 82 00 2C 表示这个 SNMP 数据部分去除前 4 个字节后的长度(44 个字节)。

- Version：SNMP 报文的版本号。这个例子中是 0，即表示为 SNMP v1。根据 4.2.1 节中介绍的 ASN.1 转换语法，十六进制表现形式窗口中被选择的数据的第 5、6 和 7 字节表示这个版本号，其中 02 表示数据类型，01 表示数据长度，00 表示实际的值。
- Community：共同体。这里的值是 public，对应的十六进制是 04 06 70 75 62 6C 69 63，其中 04 表示字符串数据，06 表示长度为 6 字节，其余表示实际的值。
- PDU type：协议数据单元(PDU)的类型。这里的值是 get-next request，对应的十六进制值是 a1。其他操作的值如下：get-request 的值为 a0，get-response 的值为 a2。再后面的三个字节是 PDU 的头部，82 00 1D 表示后面还有 29 个字节的数据。
- Request ID：请求标识。数据包中共占 4 个字节，其中第一个 02 表示整型数据，第二个 02 表示数据长度，后面两个字节 2064 表示请求标识的值，即 8292。
- Error status：差错状态，在请求时值设置为 0。十六进制表示为 02 01 00。
- Error index：差错索引，在请求时值设置为 0。十六进制表示为 02 01 00。
- Sequence：这里有两个 Sequence，都表示数据是集合类型。
- OID：请求的 OID 对象名。这里是 1.3.6.1.2.1.1。十六进制的值是 06 07 2b 06 01 02 01 01 01，其中第一个 06 数据是 MIB 变量名称类型，07 表示数据的长度，2b 表示 1.3 的和(即 $1\times40+3=0x2b$)。



• NULL Value：表示请求的 OID 对象的值，请示时为空，十六进制的值是 05 00。

SNMP 请求数据包的响应包紧跟着被捕获，即第四个数据包，双击第四个数据包，打开如图 4-16 所示的数据包分析窗口。窗口布局与图 4-15 相同。

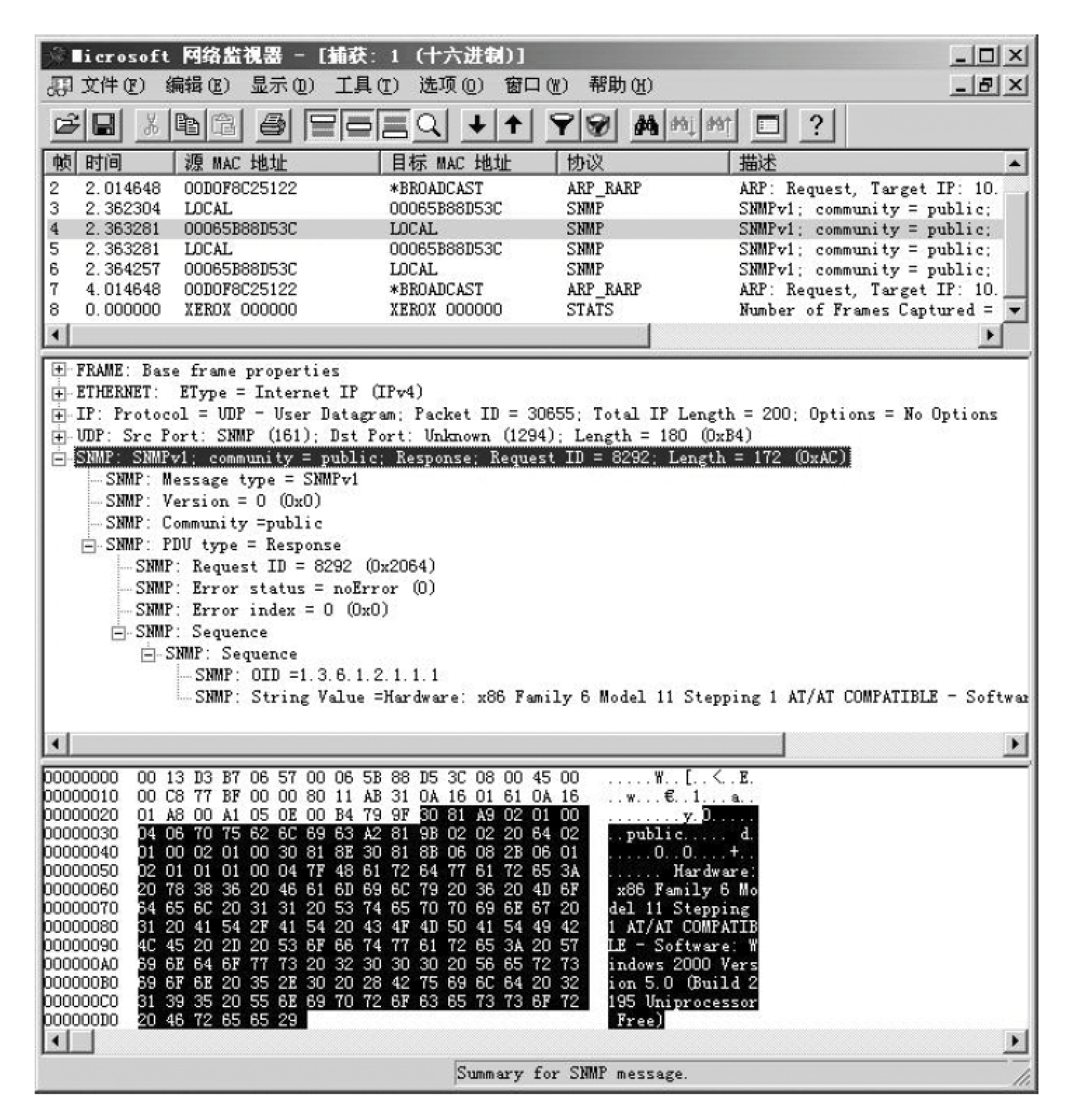


图 4-16　数据包分析窗口(2)

下面分析一下 SNMP 的数据。

• Message type：SNMP 报文类型。这个例子中是 SNMP v1 对应的十六进制的值是 30，表示后面的数据是一个复合的构造类型。再后面的十六进制值 81 A9 表示这个 SNMP 数据部分去除前几个字节后的长度(169 个字节)。
• Version：SNMP 报文的版本号。这个例子中是 0，即表示为 SNMP v1。其十六进制对应的数据是 02 01 00，其中 02 表示数据类型，01 表示数据长度，00 表示实际的值。
• Community：共同体。这里的值是 public，对应的十六进制是 04 06 70 75 62 6C 69 63，其中 04 表示是字符串数据，06 表示长度为 6 字节，其余表示实际的值。
• PDU type：协议数据单元(PDU)的类型。这里的值是 get-response，对应的十六进制值是 a2。再后面的两个字节是 PDU 的头部，81 9B 表示后面剩余数据的长度。
• Request ID：请求标识。这个值为 8292，同请求数据包中的值相同。
• Error status：差错状态。这个例子中值为 0，表示没有错误。十六进制表示为

02 01 00。

- Error index：差错索引。这个例子中值为 0，表示没有错误。十六进制表示为 02 01 00。
- Sequence：这里有两个 Sequence，都表示数据是集合类型。
- OID：请求的 OID 对象名。这里是 1.3.6.1.2.1.1。十六进制的值是 06 07 2b 06 01 02 01 01 01，其中第一个 06 数据是 MIB 变量名称类型，07 表示数据的长度，2b 表示 1.3 的和（即 1×40+3=0x2b）。
- String Value：表示请求的 OID 对象的值。

4.4 远程网络监视

远程网络监控（RMON）是对 SNMP 的一个重要增强，对监测和管理网络特别有用。远程网络监控最大的优点就在于它与现存的 SNMP 框架兼容，不需要对 SNMP 进行任何修改即可使用。

4.4.1 RMON 的基本概念

远程网络监控（RMON）是一个标准监控规范，其本质上是 IETF 定义的一组对管理信息库（MIB-2）的功能的扩展，MIB-2 只提供单个设备的管理信息，而 RMON 可以使各种网络监控器和控制台系统之间交换网络监控数据，并能够提供信息流量的统计结果和对网络参数进行分析，以便能够做出对网络的故障诊断、规划调整和性能控制。

RMON 监视系统由以下几部分构成：代理（监视器）和管理站。RMON 代理在 RMON MIB 中存储网络信息，代理可以被直接安装在网络设备中，也可以是在 PC 上运行的一个应用程序。代理只能看到流经其自己的流量，所以在每个被监控的局域网网段或广域网连接点都要设置 RMON 代理。管理站用 SNMP 获取各个代理中的数据信息，汇总后形成整个网络系统的信息。

当前 RMON 有两种版本，分别是 RMON 和 RMON2。RMON 在目前使用较为广泛的网络硬件设备中都能发现，它定义了 9 个 MIB 组服务于基本远程网络监控；RMON2 是 RMON 的功能扩展，其主要针对数据链路层以上各 OSI 模型层进行监控。

1. 远程网络监视的目标

RMON 定义了远程网络监控的管理信息库，以及 SNMP 管理站和远程网络监视器之间的接口，一般 RMON 的目标只是监视子网范围内的通信，从而减少管理者和代理之间的通信负担。RMON 具有下列目标。

- 离线操作：必要时管理者可以停止对监控器轮询，有限的轮询可以节省网络带宽和通信费用。即使不受管理者查询，监视器也要持续不断地收集子网故障、性能和配置方面的信息，统计和积累数据，以便管理者查询时能够及时提供相关的管理信息。另外，在网络系统出现异常情况时，监视器也能及时向管理者报告。
- 主动监视：如果监视器有足够的资源，通信负载也容许，监视器可以连续地或周期性地运行诊断程序，查询并记录网络系统的性能参数，在子网出现失效时通知



管理者，给其提供有效的诊断故障信息。
- 问题检测和报告：如果主动监视消耗网络资源太多，监视器也可以被动地获取网络数据，可以配置监视器，使其连续观察网络资源的消耗情况，记录随时出现的异常事件，并在出现错误事件时通知管理者，以便管理者做出相应的反应。
- 提供增值数据：监视器可以分析收集到的子网数据，从而减轻管理者的计算任务。
- 多管理站操作：一个互联网可能有多个管理站，这样可以提高可靠性，或是分步地实现各种不同的网络管理功能。监视器可以配置为并发的工作模式，为不同的管理站提供不同的信息。

需要注意，不是每一个监视器都能实现上述所有目标的，只是 RMON 的规范提供了实现这些目标的基础结构和理论依据。

2. 表管理操作原理

在 SNMP 管理框架中，对表操作的规定很不完善，增加和删除表行的操作是不明确的。这种模糊性常常是用户提问的焦点和抱怨的根源。RMON 规范包含了一组文字约定和过程规则，在不修改、不违反 SNMP 管理框架的前提下提供了清晰准确并有规律性的行增加和行删除操作。

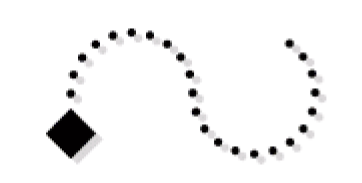
3. 多管理站访问

RMON 监视器应允许多个管理站并发地访问，当多个管理站同时访问时可能出现下列问题：
- 多个管理站对资源的并发访问可能超过监视器的能力；
- 一个管理站可能长时间占用监视器资源，使得其他管理站无法访问；
- 占用监视器资源的管理站可能发生崩溃，但是其没有释放占用的资源。

对于上述问题，RMON 提出了解决问题的方法：
- 管理站能认得自己所属的资源，也知道自己不再需要的资源；
- 网络管理操作员可以知道管理站占有的资源，并决定是否释放这些资源；
- 一个被授权的网络操作员可以单方面地决定是否释放其他操作员所占用的资源；
- 如果管理站经过了重启动过程，它应该首先释放不再使用的资源。

4.4.2　RMON 的信息管理库

RMON MIB 由一组统计数据、分析数据和诊断数据构成，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商的远程网络分析功能。RMON 规范定义了管理站信息库 RMON MIB，它是 MIB-2 下面的子树，其 OID 为.iso.org.dod.internet.mgmt.mib-2.rmon(.1.3.6.1.2.1.16)。RMON MIB 共分为 9 个组，存储在每一组中的信息都是监视器从一个或几个子网中统计和收集的数据，这 9 个组分别是：
- 统计量组(statistics)，提供了一个以太网状态表，标识子网的统计信息，大部分是计数器。
- 历史组(history)，存储的是通过固定间隔取样所获得的子网信息数据，其由历史控制列表和以太网历史表组成。



- 报警组(alarm),其由一个表组成,该表定义了监视的变量、采样区间和阈值。报警类型有两种:absolutevalue 表示直接与阈值比较;datavalue 表示相减后比较,校正量报警。
- 主机组(hosts),收集新出现的主机信息,内容与接口组同。
- 主机最大值组(host Top n),记录某组参数最大的 n 台主机的有关信息,信息来源于主机组。
- 矩阵组(matrix),记录子网中主机之间的通信量,信息以矩阵形式存储。
- 过滤器组(filter),其可以通过过滤选择出某种指定的特殊分组,这个组定义了两个过滤器:数据过滤器按位模式匹配;状态过滤器按状态匹配。
- 捕获组(capture),建立一组缓冲区,用于存储从通道中捕获的分组,其由控制表和数据表组成。
- 事件组(event),其作用是管理事件,由事件表和 log 表组成,前者定义事件的作用,后者记录事件出现的顺序和时间。事件是由 MIB 中其他地方的条件触发的,事件也能触发其他地方的事件。产生事件的条件在 RMON 其他组中定义,如报警组和过滤组都可以指向事件组的索引项。时间还能使事件组存储有关信息,甚至引起代理进程发送陷入消息。

RMON 组的组成图如图 4-17 所示。一般的交换机至少支持 4 组(即统计量组、历史组、报警组和事件组)。

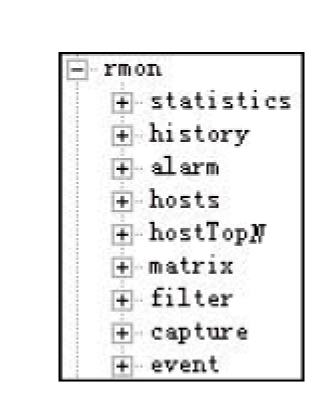


图 4-17　RMON 组的组成图

这 9 个功能组都是任选的,但实现时有下列关联关系:

- 实现警报组时必须实现事件组。
- 实现主机最大值组时必须实现主机组。
- 实现捕获组时必须实现过滤组。

4.4.3　RMON2 信息管理库

RMON 主要监测和控制 OSI 模型中的物理层和数据链路层,而 ROMN2 主要应用于 OSI 模型中数据链路层以上各层,主要监控 IP 流量和应用程序层流量。RMON2 允许网络管理应用程序监控所有网络层的信息包,这与 RMON 不同,后者只允许监控数据链路层及其下层的信息包。

RMON2 监视 OSI 模型中第三层到第七层的通信数据,其能够对数据链路层以上的分组进行译码,这使得监视器可以管理网络层以上协议,包括 IP,因而能了解分组的源和目标地址,能知道路由器负载的来源,使得监视的范围扩大到局域网之外。监视器也能监视应用层协议,如电子邮件协议、文件传输协议、HTTP 等,这样监视器就可以记录主机应用活动的数据,可以显示各种应用活动的图表,这些对网络管理人员都是很重要的信息。

RMON2 在 RMON MIB 基础上增加了 9 个功能组。

- 协议目录组:提供各种网络协议的标准化方法,使得管理站可以了解监视器所在子网运行什么协议。协议目录是一种简单的便于共同建立 RMON2 应用程序、实现 RMON 代理的途径,这对于应用程序和代理出自不同的提供商的情况尤其

重要。

- 协议分布组：提供每个协议产生的通信统计数据，将监测器收集的数据转换为正确的协议名，从而可以显示给网络管理者。
- 地址映像组：IP 地址与 MAC 地址的映射表。MAC 层的地址与网络层的地址之间的转换使得读和记忆变得容易，地址转换不仅为网络管理者提供了帮助，而且它支持 SNMP 管理平台并引入了改进的拓扑布局转换。
- 网络层主机组：收集网络上主机的信息。
- 网络层矩阵组：网络上源和目标的通信情况。
- 应用层主机组：收集每个应用的通信情况。
- 应用层矩阵组：统计应用协议之间的通信情况。
- 用户历史组：周期性地收集统计数据，这一特性使网络管理者能够配置系统中的任何历史记录，例如，在指定文件服务器或路由器对路由器的连接上的特殊历史记录。
- 监视器配置组：定义了监视器标准参数的集合，RMON2 的这一特性使某提供商的 RMON 应用程序能够配置其他提供商的 RMON 探测器。

RMON2 还引入了两种与对象索引有关的新功能，增加了 RMON2 的能力和灵活性，这两种功能分别是：外部对象索引和时间过滤器索引。

本章小结

本章主要讲述了基于简单网络管理协议（SNMP）的网络管理内容和管理信息库（MIB）的概念及组成，重点讲解了 SNMP 数据单元和其操作功能，并给出了一些示例，最后对远程网络监控（RMON 和 RMON2）进行了简单的讲解。因为学时限制，在教材中没有介绍 SNMP 的全部内容，感兴趣的读者可以参阅其他教材。

本章习题

1. ISO 定义的网络管理有哪几个功能？
2. 管理信息库第 2 版（MIB-2）中有 9 个功能组，分别是什么？
3. 简单网络管理协议（SNMP）有哪几个操作？
4. 远程网络监控（RMON）的功能是什么？

第 5 章

基于 SNMP 的网络管理系统

【本章重点】

掌握基于 SNMP 网络管理的概念和功能。掌握 SiteView NNM 的拓扑图管理、设备管理、IP 资源管理、警告管理和检测报表管理等技术。

计算机网络技术的迅猛发展,给网络管理提出了严肃的课题。如何有效地管理网络中数量越来越多、异构性越来越强的网络设备,使计算机网络运行的可靠性、安全性变得越来越强,成了网络管理者对网络管理系统的基本要求。而网络设备供应商对 SNMP 的支持,为这种实现提供了可能,本章将对此进行探讨。

5.1 基于 SNMP 的网络管理系统基础知识

计算机网络管理系统就是管理网络的软件系统。计算机网络管理就是收集网络中各个组成部分静态、动态的运行信息,并在这些信息的基础上进行分析和作出相应的处理,以保证网络安全、可靠、高效地运行,从而合理地分配网络资源、动态地配置网络负载,优化网络性能、减少网络维护费用。

1. 网络管理系统的基本构成

一个典型的网络管理系统包括 4 个要素:管理应用程序、管理代理、管理信息库、代理服务设备,如图 5-1 所示。

管理应用程序:它是实施网络管理的实体,驻留在管理工作站上。它是整个网络系统的核心,完成复杂网络管理的各项功能。网络管理系统要求管理代理定期收集重要的设备信息,收集到的信息将用于确定单个网络设备、部分网络或整个网络的运行状态是否正常。

管理代理:网络管理代理是驻留在网络设备(这里的设备可以是 UNIX 工作站、网络打印机,也可以是其他网络设备)中的软件模块,它可以获得本地设备的运转状态、设备特性、系统配置等相关信息。网络管理代理所起的作用是:充当管理系统与管理代理软件驻留设备之间的中介,通过控制设备的管理信息数据库(MIB)中的信息来管理该设备。

管理信息库:它存储在被管理对象的存储器中,管理库是一个动态刷新的数据库,它

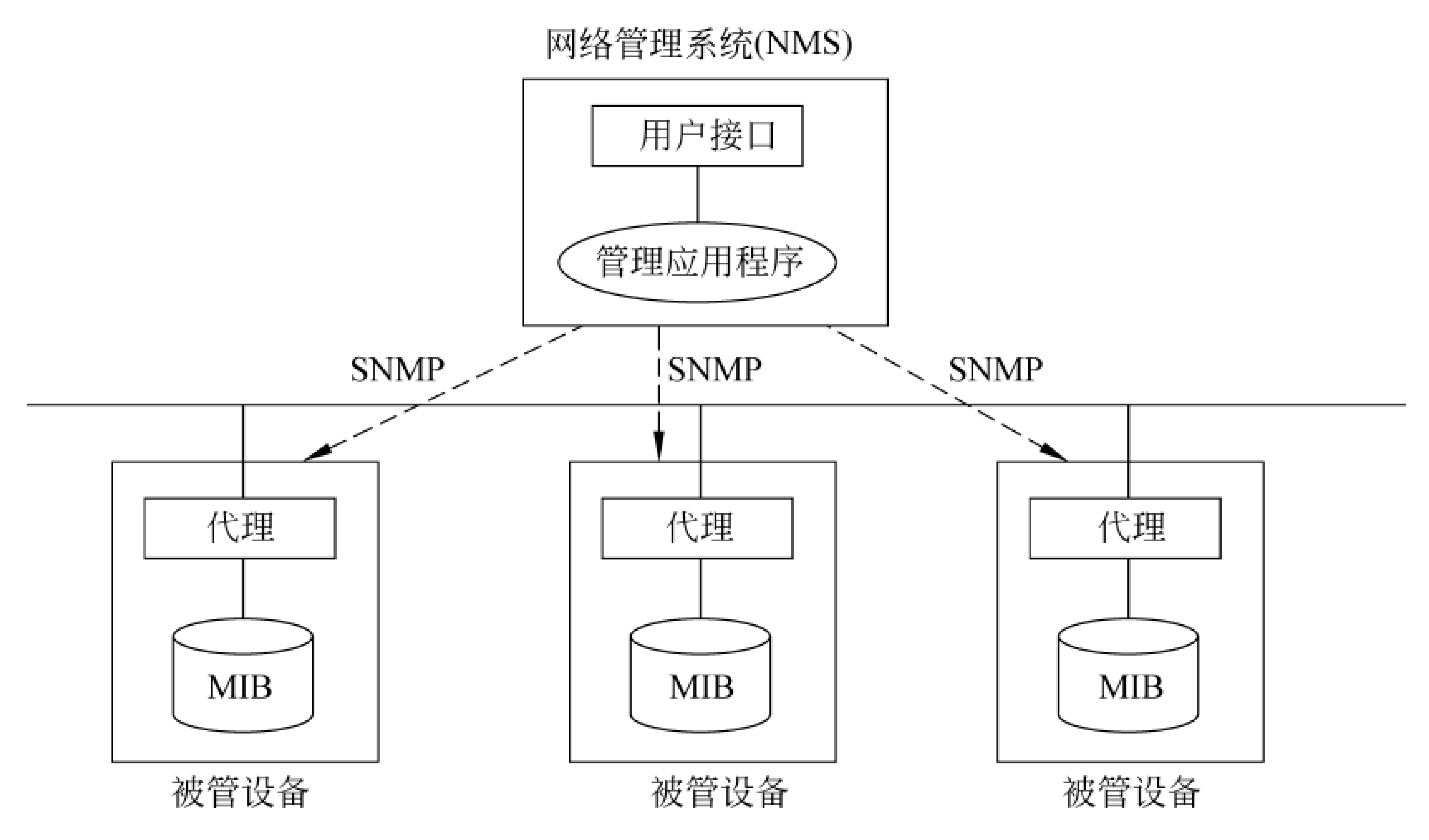


图 5-1　网管系统构成要素

包括网络设备的配置信息,数据通信的统计信息,安全性信息和设备特有信息。这些信息被动态地送往管理器,成为网络管理系统的数据来源。

代理服务设备:代理设备在标准网络管理软件和不直接支持该标准协议的系统之间起桥梁作用。利用代理设备,不需要升级整个网络就可以实现从旧协议到新版本的过渡。

2. 网络管理系统的体系结构

网络管理系统根据网络管理所采用的工作方式不同,通常分为两种结构:一种是采用以平台为中心的工作模式,通常称为集中式体系结构,这种工作模式把单一的管理者分成管理平台和管理应用两部分,管理平台的主要作用在于信息的收集和处理,管理应用则是把管理平台处理过的信息进行再分析,从中得出可以进行决策的信息,并用以发出指令,还可以借助这些再处理的信息执行更高级的功能。

另一种体系结构是非集中式的。层次方式和分布式是这种网络管理体系结构的主要内容。其中层次方式是指把整个管理网络分为一个个独立的域,然后以域为单位,在每个域上设立一个管理者,这个管理者可以是现实中的人,也可以是一个虚拟化的管理者,管理者借助管理员设置的密钥或者其他登录方式访问管理界面,对网络进行管理,管理者不必是一个固定的对象,但必须是掌握了管理员协议的,不存在任何危及系统安全隐患的才可以登录管理界面,否则便是非法入侵系统。

管理员之间一般不直接进行通信联系,而是通过上层的 MOM。层次方式可以通过增加一级 MOM 的方式,将层次不断加深,相对来说具有一定的伸缩性。

分布式是指将整个管理系统分为多个管理方,它们之间的地位和作用是对等的,同时存在于网络中,每个管理者都对系统中的一个特定部分进行管理,他们之间可以相互通信或通过高级管理者进行协调。

在计算机网络管理中,选择哪种管理体系结构,主要应该根据实际需要来确定。目前,随着网络管理方式的不断发展,一种融合两种体系优点的新的网络管理结构体系正在探讨中,目前在技术上还不够成熟,相信在不久的将来,这种新的网络管理结构体系必将

随着技术的发展而日趋成熟并得到广泛的运用。

3. 计算机网管系统的发展趋势

现在的计算机网络管理系统开始向应用层次渗透。传统的计算机网络管理系统所注意的对象就是处在网络层的各种网络设备,利用 SNMP 来控制和管理设备,以设备或者设备集为中心。现在用户在网上的应用增多,应用对网络带宽的要求也越来越高了。

其中有一些应用服务要求对时间敏感的数据传输,如实时音频视频的传输等,而有一些数据则对时间敏感度不高。因此,在现有的网络带宽有限的情况下,为了更好地利用带宽资源,必须改变原来不区分服务内容的传输,而是根据服务的内容,给各个应用提供高质量的服务,这也就是 QoS(Quality of Services)。网络管理吸收了这样的思想,开始把自己的控制力从网络层渗透到了应用层,RMON2 就在这方面进行了尝试,这也是网络管理系统的一个重要的变化。

然而,尽管网络管理技术多种多样、各具特色,但是随着标准化活动的开展及系统互联的需要, 网络管理发展有以下趋势。

(1) 实现分布式网络管理

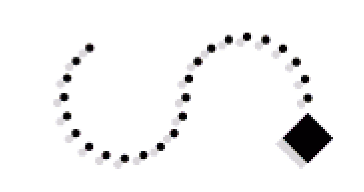
分布式对象的核心是解决对象跨平台连接和交互的问题,以实现分布式应用系统,像 OMG 组织提出的 CORBA 就是较理想的平台。分布式网管就是设立多个域管理进程,域管理进程负责管理本域的管理对象,同时进程间进行协调和交互,以完成对全局网的管理。这样,不仅减少了中央网管的负荷,而且减少了网管信息传递的时延,使管理更为有效。当前,分布式技术主要从两个方面进行研究:一个是利用 CORBA 技术;另一个是利用移动代理技术。

基于 CORBA 技术的网络管理,目前处于研究阶段;移动代理技术也仅在各个区域进行研究。何时推向市场和走进网络管理应用还是个未知数。因此,在未来的近期使用中,可采用集中分布式的网络管理模型具体实现管理集中、数据采集分布的管理功能。即一个管理站进行数据呈现和管理,在数据采集这种消耗大量内存和占用大量带宽方面采用分布式方法获得。实现方法为管理站具有分发代码的功能,在网络层发现网关后,同时向该网关发送代码实现该子网的各项数据采集,以此减轻管理站的负担和减少管理端网络拥塞。

(2) 实现综合化网络管理

综合化网络管理要求网络管理系统提供多种级制的管理支持。通过一个操作台实现对各个子网的透视;对所管业务的了解以及提供对故障的定位和排除的支持,即实现对互联的多个网络的管理。随着网络管理的重要性越来越突出,各种各样的网络管理系统应运而生。这些管理系统有管理 SDH 网络的,有管理 IP 网络的,等等。

一方面,这些网络管理系统所管理的网络存在互联或互相依赖的关系;另一方面,存在多个网管系统,相互独立,分管网络的不同部分,甚至会同时存在多个相同内容的网管系统,它们来自多个厂家,分别管理着各自的设备。这就大大增加了网络管理的复杂性。像网络电视,就需要管理几个方面:数字干线传输、光缆线路、前端及分前端级供电房供电、空调环境的监测维护、数据库及数据交换信息服务、前端节目源及视频、音频设备和 HFC 综合接入网等。



这些被管对象作为一个网管系统的被管对象是不实际的，因为不仅设备的种类不同，而且其特性也大不相同，并且它们之间还有一定的关系，针对这种问题，可把它们分割为不同的网管系统，然后在高层采用一个综合的网管系统，以便于管理。综合网络管理系统的实现有两种方案：一种是针对已经建立起的各个专用子网的管理系统的不同情况，在此基础上建立综合网络管理系统；另一种是直接建立一个综合网络管理系统。而在我国，网络电视还没有成熟，所以宜采用第二种方法，因此，未来的网络管理须重点向综合化发展。

(3) 实现对业务的监控功能

传统网管都是针对网络设备的管理，并不能直接反映出设备故障对业务的影响。目前有些网管产品已经实现了对进程的监控，但是有些服务，虽然服务已经终止，但是进程仍然存在，并不能明确显示对服务监控。对于客户来说，他们注重所得到的服务，像节目的多少、节目的质量等，因此，对服务、业务的监控将是网管进一步的管理目标。

(4) 实现智能化管理

支持策略管理和网络管理系统本身的自诊断、自调整。采用人工智能技术进行维护、诊断、排除故障及维护网络运行在最佳状态成为必然趋势。当网络管理和用户需求不直接联系；网络性能下降等网络运行性能变化时，必须用智能化方法对涉及性能下降所相关的网络资源进行监控，执行必要的操作。

(5) 实现基于 Web 的管理

通过使用 Web 浏览器在网络的任何节点上去监测、控制网络及各子网的管理功能。基于 Web 的管理以其统一、友好的界面风格，地理和系统上的可移动性以及系统平台的独立性吸引着越来越多的用户和开发商。

目前的计算机网络管理功能仅实现了该网络管理系统功能开发和应用的一部分，离整个计算机网络管理功能的实现还有一定的差距，今后可在这方面作进一步研究和开发，以完善其管理。

4. 常见的基于 SNMP 的管理软件

(1) 惠普公司的 HP OpenView

HP OpenView 是 HP 公司开发的网络管理平台，是一种当前网络管理领域比较流行的、开放式、模块化、分布式的网络/系统管理解决方案。它集成了网络管理和系统管理的优点，并把两者有机地结合在一起，形成了一个单一而完整的管理系统。作为业界领先的网络管理平台，Network Node Manager 和 Network Node Manager Extended Topology 共同构成了业界最为全面、开放、广泛和易用的网络管理解决方案。该解决方案可以管理交换式第二层和路由式第三层综合环境。

Network Node Manager 和 Network Node Manager Extended Topology 可以让用户知道自己的网络什么时候出了问题，并帮助用户在这个问题发展成为严重故障之前解决它。与此同时，它们还可以帮助用户智能化地采集和报告关键性的网络信息，以及为网络的发展制订计划。Network Node Manager 可以自动地搜索用户的网络，帮助用户了解自己的网络环境。对第三层和第二层环境进行问题根本原因分析；提供故障诊断工具，帮助用户快速解决复杂问题。收集主要网络信息，帮助用户发现问题并主动进行管理。为

用户提供即时可用的报告，帮助用户提前为网络的扩展制订计划。让网络维护人员、管理人员和客户可以通过 Web 从任何地方进行远程访问。通过它的分布式体系管理大型的网络。提供有针对性的事件视图，以便迅速地发现和诊断问题。提供一个增强的 Web 用户界面和一些用于动态更新设备状态的新视图(这种功能需要采用 Network Node Manager Extended Topology)。提供可以显示设备之间复杂关系的视图等其他功能。

(2) Cisco 公司的 Cisco Works

Cisco Works 是 Cisco 公司为网络系统管理提供的一个基于 SNMP 的管理软件系列，它可集成在多个现行的网络管理系统上，如 SunNet Manager、HP Open View 以及 IBM Net View 等。Cisco Works 为路由器管理提供了强有力的支持工具，它主要为网络管理员提供以下几个方面的应用：可执行自动安装任务，简化手工配置。提供调试、配置和拓扑等信息，并生成相应的 Drofile 文件。提供动态的统计、状态和综合配置信息以及基本故障监测功能。搜集网络数据并生成相应的图表和流量趋势以提供性能分析。具有安全管理和设备软件管理功能。

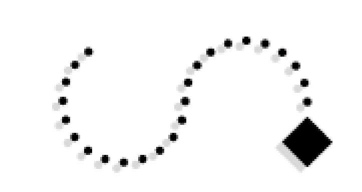
(3) Solarwinds

Solarwinds 改变了各种规模的公司的网络监控、管理模式，和同类软件 HP OpenView、BMC 相比，功能上虽然没有那么强大，但其也有非常大的优势。首先价格较便宜，这是各个企业考虑的重要因素之一。其次操作简单、配置方便，不像 HP OpenView 之类的软件需要专门人员进行配置，界面相当友好，逻辑性很强，一般的技术人员即可以操作。另外被管理设备只需开启 SNMP 即可，不必安装 Agent，不必重启，对当前业务系统无影响。同时 Solarwinds 系列网管主要分为三大功能：故障和性能管理、配置管理、网管必备工具集成。

(4) 游龙科技 SiteView 网络管理系统

SiteView 是中国游龙科技自主研发的、专注于网络应用的故障诊断和性能管理的运营级的监测管理系统，主要服务于各种规模的企业内网和网站，可以广泛地应用于局域网、广域网和互联网上的服务器、网络设备及其关键应用的监测管理。SiteView 产品包括 ITSM：IT 服务管理；ECC：综合系统管理；NNM：网络设备管理；LM：系统日志管理；EIM：互联网行为网关；DM：桌面管理；VLAN：虚拟局域网；TR069：智能设备管理。

SiteView 具有以下特点：对网络、服务器、中间件、数据库、电子邮件、WWW 系统、DNS 服务器、文件服务、电子商务等应用实现全面深入的监测；采用非代理、集中式监测模式，被监测机器无须安装任何代理软件；跨各种异构操作平台的监测。监测平台包括各种 UNIX、Linux 和 Windows NT/2000 系统；故障实时监测报警，报警可以通过 SMS、邮件、声音、电话语音卡等多种方式发送；网络标准故障的自动化诊断恢复；自动生成网络拓扑结构，快速获得并且随时更新网络的拓扑图；网络应用拓扑直观显示真实网络环境的运行状况；标准化、个性化的报表系统，可定时发送到网管人员的邮箱；智能模拟用户行为监测业务流程(如网上购书、网络报税、网上年检等)。系统采用分布式架构、支持多国语言等。



5.2　SiteView NNM 管理控制台简介

SiteView NNM 是专门针对中国网管人员开发的网络设备管理软件。它全面支持 SNMP v1、v2，方便导入 MIB 库，并提供可远程操作的设备面板图。SiteView NNM 通过动态搜索网络内的所有子网，全面呈现网络拓扑结构，实时显示网络设备、服务器和 PC 设备的运行状况和资源利用状况。SiteView NNM 由拓扑图管理、设备管理、IP 资源管理、告警管理、监测报表、日志、系统设置几个模块组成。系统具有技术领先，运行稳定的优点，同时，也是一款搜索快、数据全、功能强大、性价比高的拓扑自动发现软件。

启动程序后，登录到 SiteView NNM 的操作界面，如图 5-2 所示。SiteView NNM 是架构在 Microsoft 管理控制台上的一个系统。它通过提供在不同模块(也称为管理单元)间通用的窗口、菜单、工具栏、描述栏等，来统一和简化 SiteView NNM 中的日常系统管理任务。MMC 本身不执行管理功能，但承载了 SiteView NNM 中能够执行管理功能的各种管理单元。如图 5-2 所示，是 MMC 窗口结构和各控件的名称。



图 5-2　SiteView NNM 操作界面

(1) 标准菜单：包括 5 个菜单选项，即文件、操作、查看、窗口、帮助，它们的作用如下。

"文件"菜单可以执行磁盘清理，清理用户更改 MMC 视图时系统自动保存的配置文件。

"操作"菜单对应操作窗格，其当前可用的操作与操作窗格中的一样。

"查看"菜单作用于结果窗口，它包括添加/删除列表、大图标、小图标、列表、详细信息、自定义视图，选择这些项目，可以改变结果窗口的显示效果。

"窗口"由新建窗口、窗口排列方式、当前打开的窗口组成。当前打开的窗口有两个以上时，窗口排列方式才有效。

"帮助"菜单提供了 SiteView NNM 的帮助文档。

(2) 标准工具栏：它的具体功能如下。

返回到刚才的操作；

以当前树叶或树枝为基准，返回到上一级的树枝或根节点上；

显示/隐藏控制台树；

单击可以打开 MMC 的帮助说明；

显示/隐藏操作窗格。

(3) 控制台树。

树是 MMC 窗口左侧窗格中的层次结构，即控制台树。树显示 SiteView NNM 的全部功能模块。单击标准工具栏上的，可以显示或隐藏树。

树由根节点、树枝、树叶组成。根节点就是树中唯一的一个标记为“控制台根节点”的文件夹，树枝是 SiteView NNM 的功能模块，单击展开一个模块并查看其内容，单击则关闭，树叶是不能包含其他项目的项目类型，即树枝的最底层，也是功能模块的最底层，单击树叶，系统会在结果窗格中显示此功能的列表、文本或者图形信息。

树的快捷菜单在操作窗格中都可以找到，在本文中我们对树的快捷菜单不作阐述。

(4) 结果窗格。

它是 MMC 的中心窗格，始终显示，不能隐藏。该窗格显示控制台树中当前所选的功能模块所包含的对象和内容的有关信息，包括列表、表格、图形等。在控制台树中单击不同的功能模块时，结果窗格中的信息也会相应地发生变化。

(5) 操作窗格。

它位于 MMC 的右侧，根据控制台树中和结果窗格中当前所选的模块列出当前可用的操作，参见图 5-2 的操作窗格。通过标准菜单中的“操作”或右击要执行操作的项目，也可以访问这些操作，但上文我们已说明过，不对这两种操作方法详细讲述。单击标准工具栏上的，可以显示或隐藏操作窗格。

5.3 SiteView NNM 拓扑图管理

拓扑图管理主要通过动态搜索网络内的所有资源，全面呈现网络的拓扑结构，对网络设备的运行状态和资源状况进行实时管理。在进行正式扫描之前，为了得到理想的、完整的网络拓扑结果，必须进行扫描配置。

5.3.1 扫描配置

扫描配置包括算法配置、共同体名配置、设备信息库配置。这三项配置共同限制和约定了扫描的条件，直接影响到扫描的结果。

1. 算法配置

算法配置包括扫描算法的选择、扫描参数的设定以及扫描范围的设置。

(1) 扫描参数

单击“拓扑图管理”→“扫描配置”→“算法配置”→“扫描参数”命令，进行扫描参数设置，如图 5-3 所示。

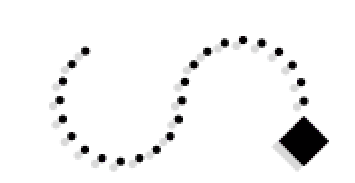




图 5-3　扫描参数设置

搜索深度：用于设置扫描时，允许的网络层次深度；

并行线程数：表示扫描时可以同时执行的最大线程数目；

重试次数：扫描时，如果访问某台设备未成功，允许重试的次数；

超时时间：指扫描设备时，允许的最大超时时间，以秒为单位；

用户在扫描网络之前可以根据具体情况对这些参数进行设置，设置完成后单击“保存”即可。

（2）扫描范围

单击“拓扑图管理”→“扫描配置”→“算法配置”→“扫描范围”命令，进行扫描范围设置，如图 5-4 所示。

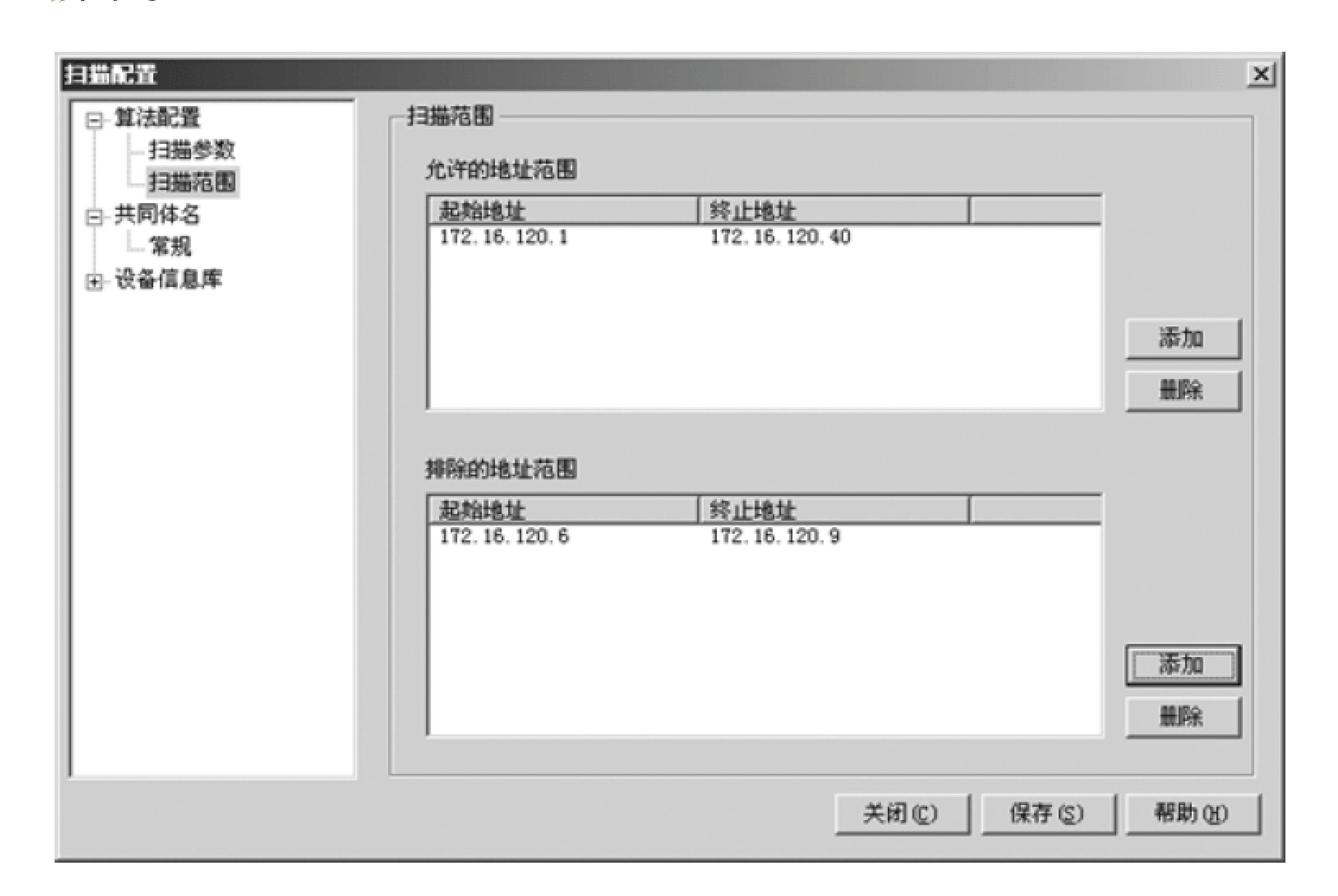
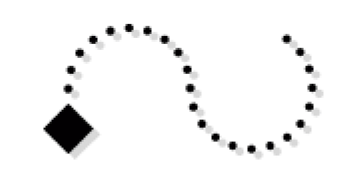


图 5-4　扫描范围设置

扫描范围分两种：一是“允许的地址范围”；二是“排除的地址范围”。“允许的地址范



围”内合适的设备会被添加到拓扑图，“排除的地址范围”是指不需要搜索的地址范围，这样可以加快拓扑图的生成速度，避免浪费系统资源。

单击“添加”，可以输入允许和排除的IP地址范围，如图5-5所示。

添加完成后，如果需要删除某条地址范围，在“允许的地址范围”和“排除的地址范围”对话框中选中需要删除的地址，单击“删除”即可实现。

在图5-4中单击“保存”，即可实现扫描范围的配置。



图5-5　输入IP地址范围

2. 共同体名配置

共同体名相当于一台设备的密码，分为被读和被写的密码，目的是在网络中起到安全防御的作用，一般由网络管理员对设备进行设置。共同体名配置分为共同体名默认设置和指定设备共同体设置，如图5-6所示。



图5-6　共同体名配置

(1) 共同体名默认设置

鉴于很多用户经常将网络设备的共同体名设置成相同的，所以我们提出默认共同体名的概念，即这个共同体名对所有设备有效，用户应该将网络中大多数设备所拥有的共同体名设置成默认，GET为读共同体名，SET为写共同体名。

在图5-6中，输入GET和SET的值，即可完成共同体名默认设置。

(2) 指定设备共同体设置

对于共同体名字与默认值不一样的设备(注意，无论是GET还是SET，只要有一处不同，就要特殊处理)，必须进行指定设置。系统提供了三种指定方法：添加、共同体名自动匹配、按范围指定，用户可根据实际情况灵活选用，简化操作过程。

① 添加。

可以添加单个设备的读写共同体名。在图5-6中，单击“添加”，打开“新增设备共同

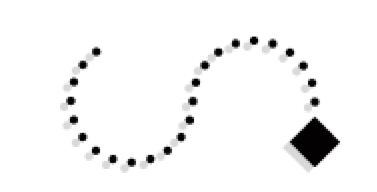




图 5-7　“新增设备共同体”窗口

体”窗口，如图 5-7 所示。

输入指定设备的 IP 地址、读共同体名(GET)、写共同体名(SET)，即可完成指定设备共同体名设置的单个添加。

② 共同体名自动匹配。

也许用户会碰到这样的麻烦：网络设备非常多，共同体名有好几个，但是具体哪台设备匹配哪个共同体名却记不清了。如果手工排查实在太麻烦了，那么就使用我们提供的这个工具——共同体名自动匹配。在图 5-6 中单击“共同体名自动匹配”，打开“共同体匹配”窗口，如图 5-8 所示。

图 5-8　“共同体匹配”窗口

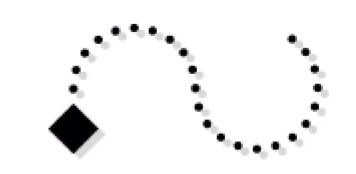
它的使用很简单，首先在需要匹配的 IP 地址范围中，添加需要查询的设备 IP 地址，可以是单个地址，也可以是一个起始段的 IP 地址，允许添加多条记录；其次在需要配备的共同体名中，添加所有可能的读共同体名(GET)；最后，选择是否仅对 Ping 响应的设备进行共同体名匹配；单击“开始匹配”，查找到的设备 IP 地址及其所对应的共同体名会显示在列表中。如图 5-8 所示，单击“确定”退出，即可实现共同体名自动匹配。

③ 按范围指定。

如果某一个 IP 段的设备读写共同体名相同，且有别于默认配置，就可以用此方法进行指定，在图 5-6 中单击“按范围指定”，打开对应窗口，如图 5-9 所示。



图 5-9　按范围指定共同体名



输入起始 IP、结束 IP、读共同体名、写共同体名，单击“确定”退出，即可实现按 IP 范围指定配置。

3. 设备信息库

设备信息库相当于设备的大集合，包含了二层交换机、三层交换机、路由器、PC 终端等设备的信息，罗列了各种设备的 SysOID 信息、厂商、型号、设备类型；包含了目前主流、非主流厂商生产的绝大部分设备，供扫描参考用。用户也可以自行添加库中没有的设备信息。

单击“设备信息库”→3Com 命令，打开设备信息库界面，如图 5-10 所示。



图 5-10　设备信息库

添加厂商：单击“添加厂商”，在弹出的添加厂商窗口中输入厂商名字，如 Dell，确定后，系统将 Dell 加入设备信息库的控制台树中，并自动排序。

添加设备：首先选择一个厂商，在打开的设备信息库界面中，用户可在最后一行空白的单元格处依次输入设备的信息，同时，系统会自动添加一行空白单元格，输入完成后，单击“保存”，即实现了设备的添加，完成了信息库的配置。

5.3.2 扫描全网

扫描配置完成后，进入正式扫描；SiteView NNM 扫描时，通过发现代理来发现设备。发现代理从一个种子节点开始，通过 SNMP 和 ICMP(Ping)两种方式，采用高效率的增量算法，多线程式地搜索整个网络，自动发现设备，生成网络拓扑结构图，同时，可以搜索到指定 IP 地址的子网络，跨越公网直接定位到下属子网。

(1) 单击“拓扑图管理”→“扫描全网”命令，打开“扫描等待”对话框，如图 5-11 所示。

扫描子网：表示只扫描子网，选择扫描子网，系统要求输入子网的地址范围，即扫描种子，如图 5-12 所示，输入完成后，系统可以自动发现并拓扑出这些子网内的所有网络设备。

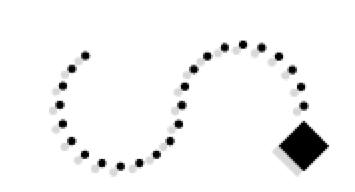




图 5-11　“扫描等待”对话框

增量扫描：在已经扫描出网络拓扑图的基础上，如果网内又添加了新的设备，则进行此扫描，以便在拓扑图上添加到新增的设备。

注意：*首次扫描时不要选择增量扫描。*

扫描算法：分为通用算法和 CDP 算法。其中通用算法适用于所有的设备扫描，CDP 算法只适用于 Cisco 的设备扫描。用户可根据网内设备的情况灵活选择合适的扫描算法，以生成最佳的拓扑图结构。

在图 5-11 中，不选择“扫描子网”，所进行的扫描就是全网扫描。单击“开始”，系统要求输入种子 IP，如图 5-13 所示指定 IP 种子后系统扫描将以该 IP 为中心进行自动拓扑发现；种子节点可以有多个且必须支持 SNMP；如果不指定 IP 种子，则系统以本机(127.0.0.1)为 IP 种子进行扫描。





图 5-12　输入子网地址范围

图 5-13　扫描 IP 种子设置

单击 >> 和 << 可以在对话框中进行 IP 种子的添加、删除。

开始扫描后，可以通过“扫描等待”对话框查看整个扫描过程，如图 5-14 所示。



图 5-14 “扫描等待”对话框

注意：扫描过程中，开始发现子网、发现设备时可以取消扫描，到分析线路时不再允许取消扫描。

(2) 扫描完毕后，单击“关闭”，系统自动开启拓扑图排版功能，弹出“排版选项”对话框，如图 5-15 所示。

系统提供了 4 种排版风格，默认为普通排版，用户可根据个人喜好或者网内设备拓扑的实际情况自行选择排版风格。

选定风格，在此以普通排版为例，单击“确定”，系统在拓扑图结果窗口中显示出拓扑结构图，如图 5-16 所示。

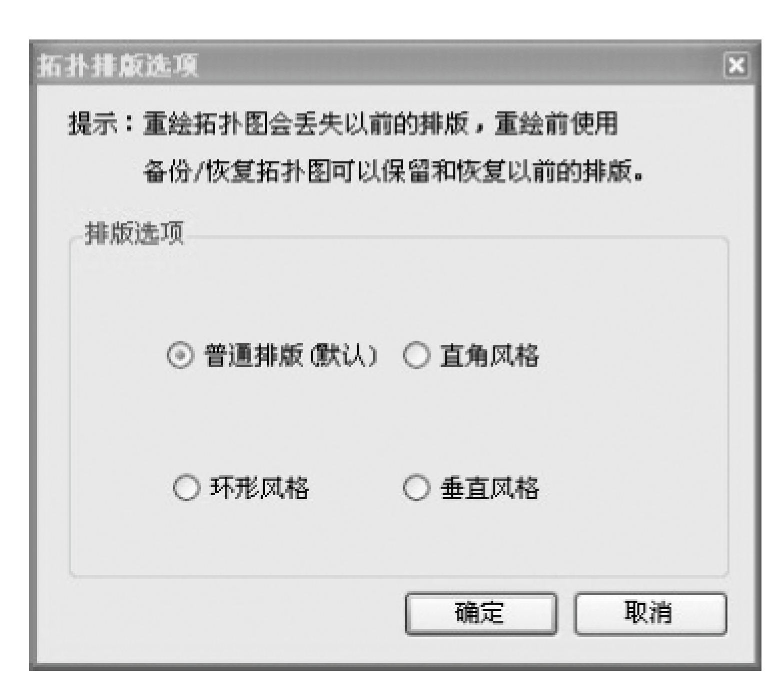


图 5-15 拓扑图排版格式

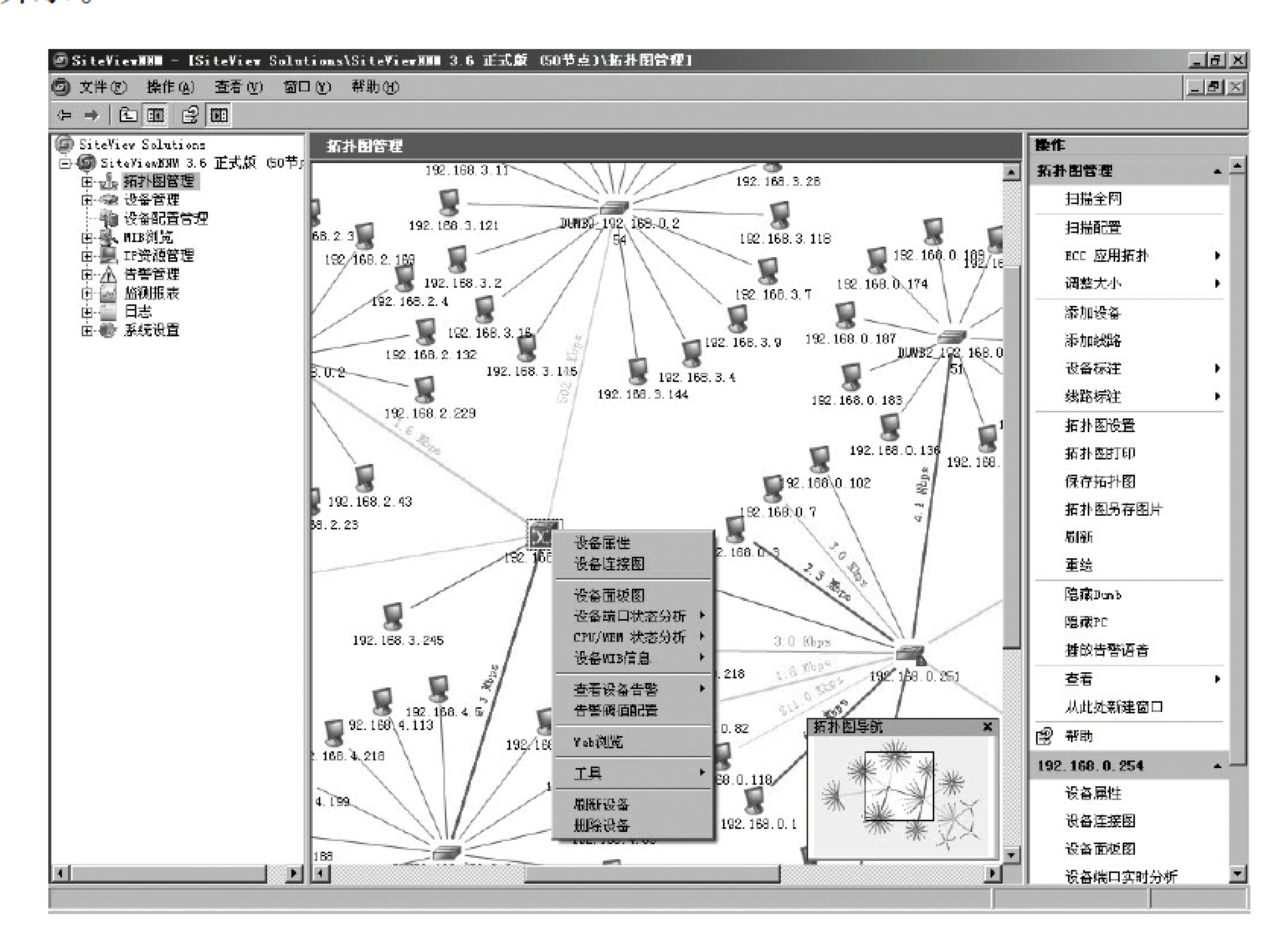
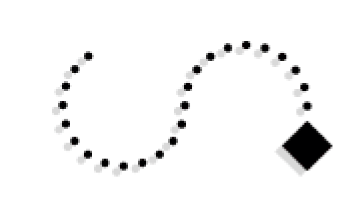


图 5-16 网络拓扑结构图



5.4　SiteView NNM 设备管理

此模块用于对全网内的各种设备进行统一的资源管理，它记录了所有的设备及设备的各种信息，实现对设备性能和运行状态的实时监控、分析。为便于对设备的有序管理，系统采用分类管理的办法。系统默认的分类方式是设备类型。用户可以根据网络的特殊情况，自行添加分类；如可按设备所在部门、按设备所在的地理位置等进行分类。

5.4.1　设备列表

系统统计了设备的数量、设备的主要信息，并按设备的类型进行了分类排列以供用户查看，打开此表可对全网内的设备情况有一个大致的了解。单击“设备管理”→“全网设备统计”，打开窗口，如图 5-17 所示。它同时具有刷新、显示过滤和导出 Excel 三个子功能。

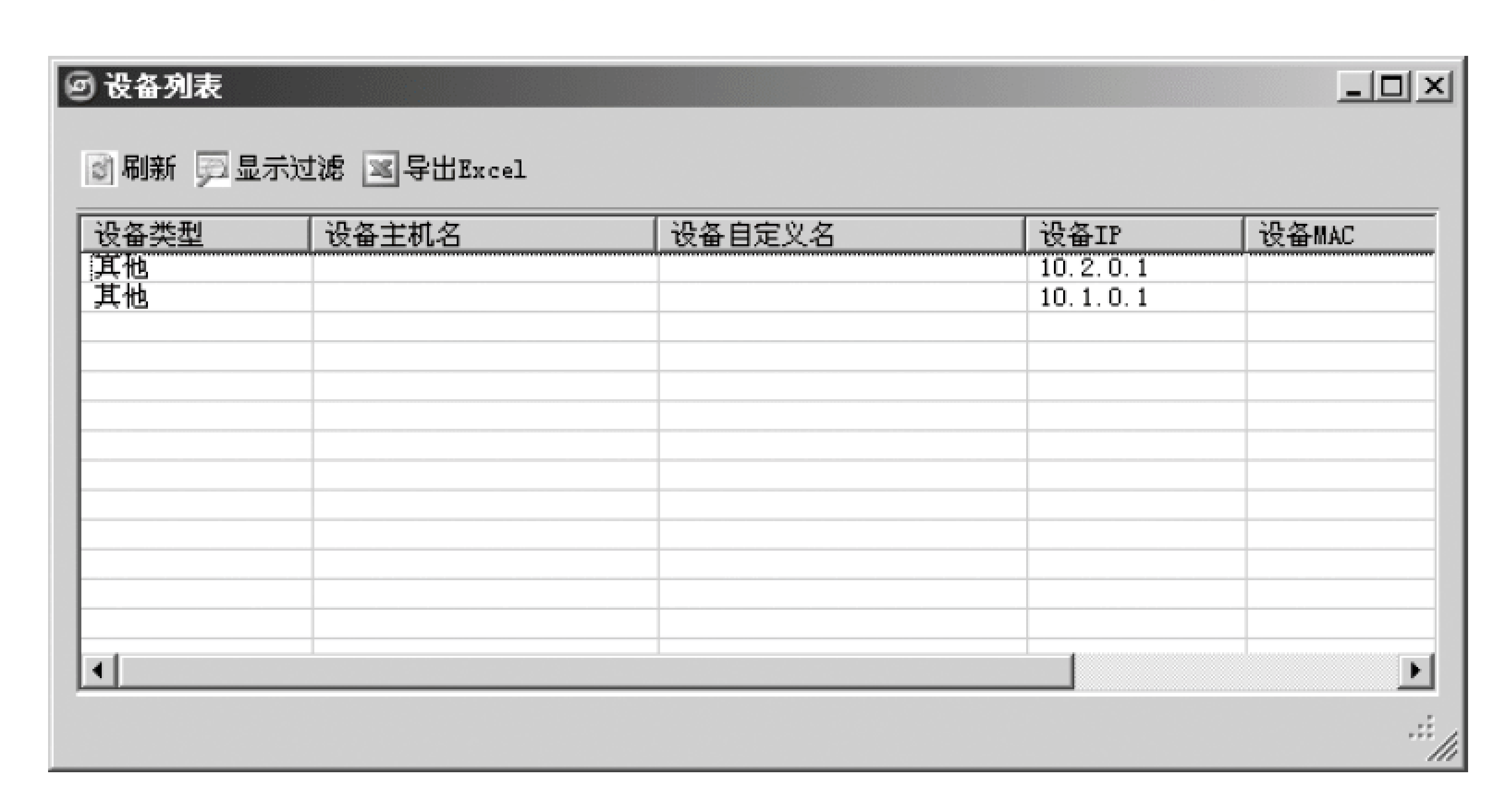


图 5-17　“设备列表”窗口

5.4.2　设备属性查看

设备管理最重要的一个模块，可以实时查看所有设备的属性及各种信息，监控设备性能和运行状况。以下我们将一一阐述，仅以二层交换机为例。

单击“设备管理”→“设备类型”→“二层交换机”命令，打开二层交换机的设备列表窗口，在此窗口中，选中一台设备，单击菜单进行相关操作，如图 5-18 所示。在操作窗格可以进行设备属性设置、设备定位、MIB 信息和设备面板图查看等相关操作。

1. 设备属性

单击“设备属性”，打开的窗口如图 5-19 所示。设备属性分为“一般信息”和“端口信息”两个 TAB 页，在“一般信息”中，用户可以查看详细的设备记录和信息，并可以自定义设备名称和设备备注；“端口信息”TAB 页列出了设备的所有端口号、端口类型、管理状态、端口描述，用户可以实时了解设备端口的工作和管理状态。

2. 设备定位

此功能可以帮助用户查看当前设备所连接的上级设备以及连接的端口号，提供设备

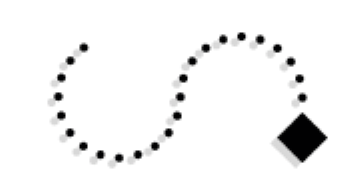


图 5-18 设备选定

图 5-19 “设备属性”窗口

IP 和设备 MAC 两种类别进行定位。如图 5-20 所示，单击“定位”按钮，系统即可显示定位结果。

二层交换机、三层交换机、路由器、服务器，这 4 种类别的设备还可以定位到拓扑图中，单击在拓扑图中显示，系统会自动返回拓扑图中，以颜色和边框显示当前设备在拓扑图中的位置，及其与其他设备的连接情况。如果该设备不在拓扑图中，系统也会给出相应



提示(注意：必须要先定位成功,才能在拓扑图中显示)。

图 5-20　设备定位

对于 PC 终端的设备定位,系统有特殊的处理。如果主拓扑图设置为"显示 PC 终端",那么,当 PC 终端定位成功后,可以直接在拓扑图中显示出来;反之,PC 终端将定位到设备连接图中,以 192.168.0.19 为例,如图 5-21 所示和图 5-22 所示。



图 5-21　设备定位

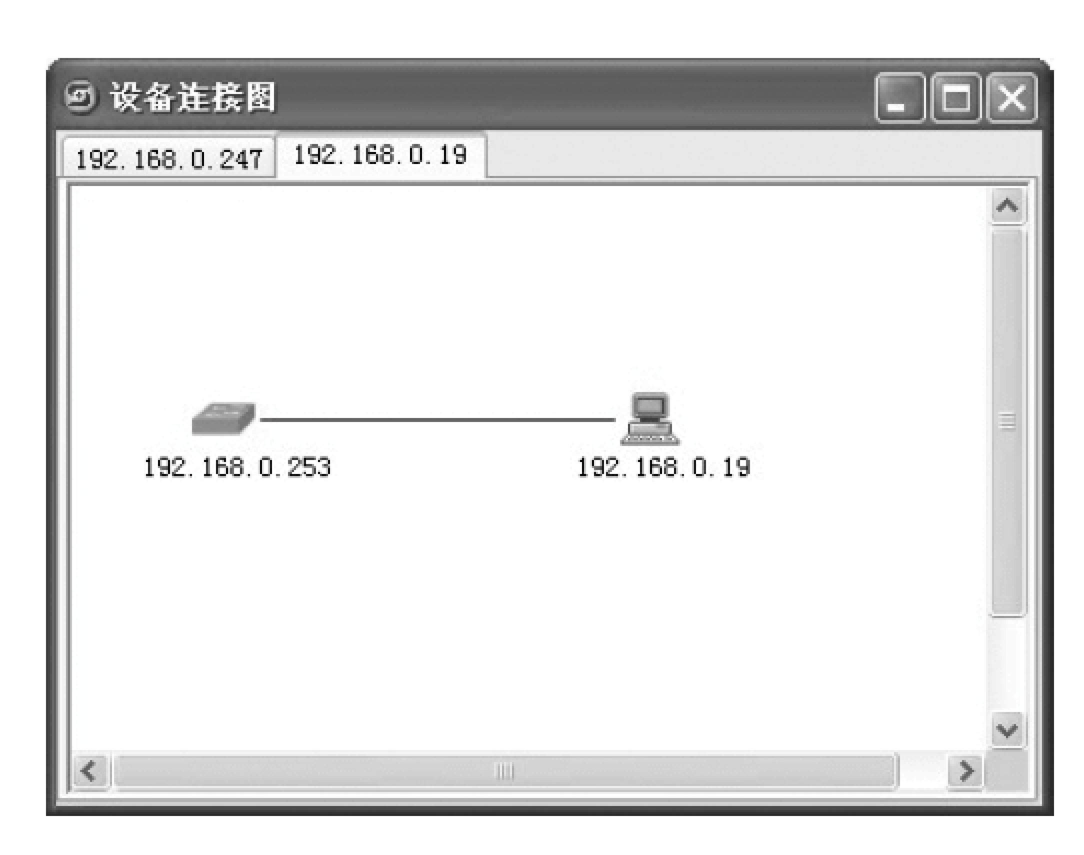


图 5-22　设备定位的拓扑图

3. MIB 信息

利用此功能用户可查看网管设备的 MIB 信息，如图 5-23 所示。MIB 信息提供 6 种信息数据，分别是接口表信息、路由表信息、转发表信息、ARP 表信息、CDP 表信息、IP 表信息，单击信息表下拉框可进行选择；MIB 信息提供“不刷新——600 秒”的时间间隔，随时更新数据，了解其变化及变化趋势，单击刷新间隔下拉框可进行选择；单击[...]可选择设备。

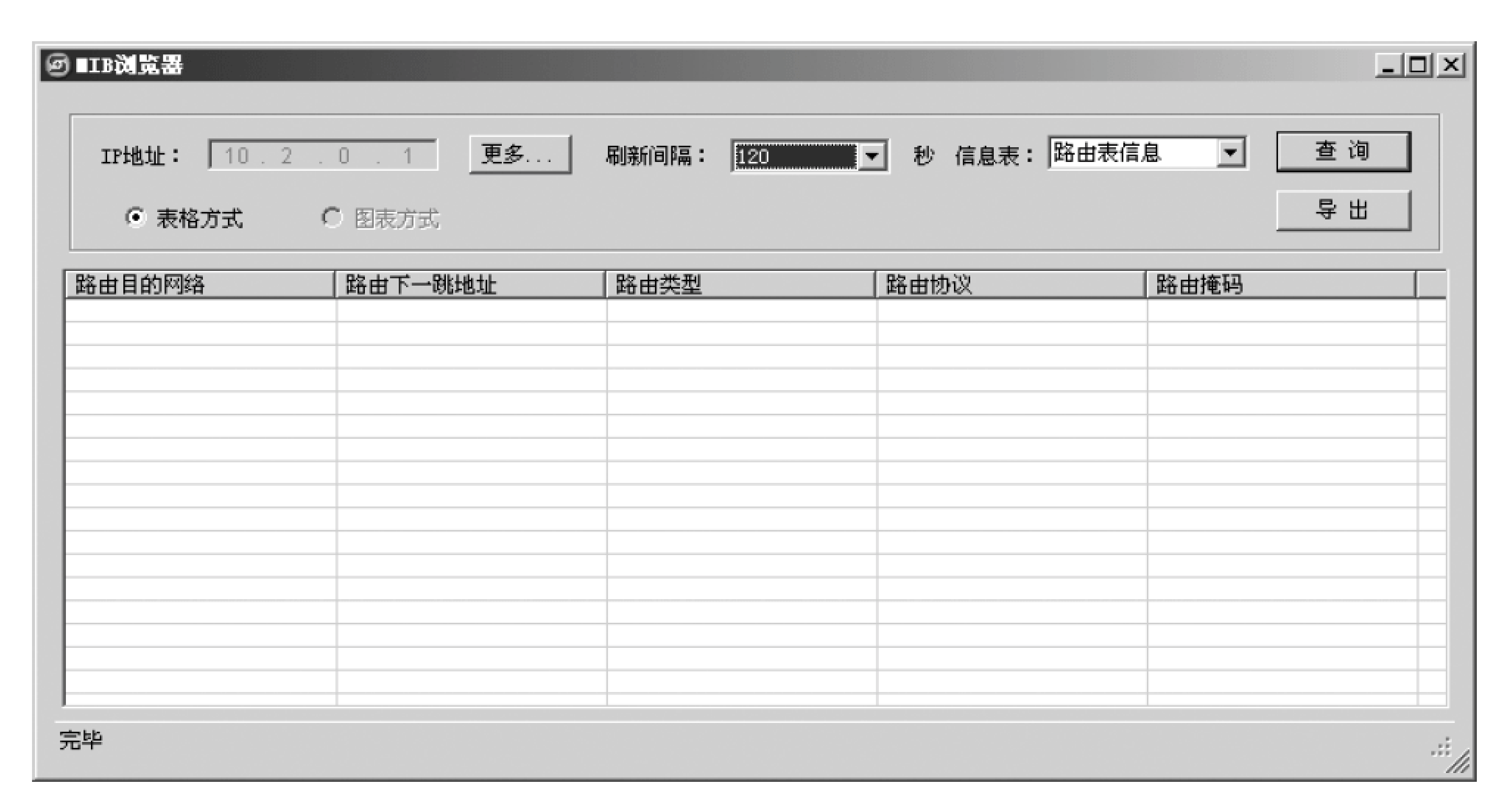


图 5-23 MIB 信息

4. 设备面板图

提供设备的真实面板图，在面板图上用户可以很直观地查看当前设备所有的端口信息。首先，系统设置了不同颜色表示端口的工作状态：UP 或者 DOWN；其次，将鼠标光标停留在端口上，可以查看到更详细的端口信息：端口索引、端口描述、接口索引、端口状态、管理状态；一目了然，如图 5-24 所示。

右击端口，打开快捷菜单，可以查看端口流量、端口属性，根据网络中的具体环境和要求对端口进行打开/关闭的操作，如图 5-25 所示。



图 5-24 设备面板

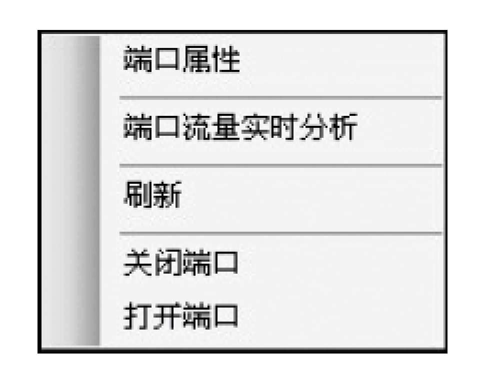
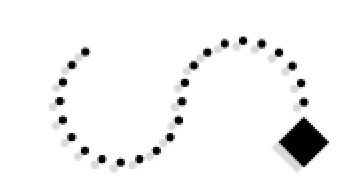


图 5-25 端口快捷菜单



5.5　SiteView NNM IP 资源管理

实现对全网 IP 地址进行有效的监控和资源管理，包括子网、IP-MAC 基准数据、IP-MAC 异动查询三个模块。

5.5.1　子网

提供网段内 IP 资源查询、管理，网段分析和统计，自动探测各网段的 IP 地址使用情况。全网扫描后，系统自动将扫描出来的子网结果显示在此模块中，以网段为控制台树枝的方式罗列出来，每扫描一次，子网模块就更新一次。单击“IP 资源管理”→“子网”，打开如图 5-26 所示的窗口。



图 5-26　“子网列表”窗口

1. 子网统计

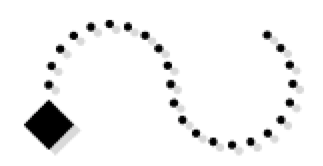
系统将子网内各网段的数据进行了完整的统计，包括子网总数、子网 IP、子网掩码、可用 IP 总数，可分配 IP 数。系统提供列表和图形两种展示方法。

单击“IP 资源管理”→“子网”→“子网统计”命令，打开“子网统计”对话框，如图 5-27 所示。

2. 网段

单击“IP 资源管理”→“子网”→192.168.0.0/24 命令，可以一目了然地查看此网段内的 IP 地址使用情况，其详细信息包括 IP 地址、设备名称、设备类型、MAC 地址，如图 5-28 所示。

由图 5-28 可见，单击 IP 地址列表中的其中一台设备，可以打开菜单或者右击打开快



子网统计

列表展示 图形展示

子网总数(14)：

子网IP	子网掩码	可用IP总数	已分配IP数
192.168.0.0	255.255.255.0	255	52
192.168.10.0	255.255.255.0	255	1
20.0.0.0	255.255.255.0	255	6
192.168.3.0	255.255.255.0	255	25
99.1.1.0	255.255.255.0	255	2
192.168.8.0	255.255.255.0	255	5
192.168.200.0	255.255.255.0	255	1
192.168.0.0	255.255.0.0	65535	87
192.168.1.0	255.255.255.0	255	2
100.100.100.0	255.255.255.0	255	1
10.8.0.0	255.255.255.0	255	2
192.168.6.0	255.255.255.0	255	1
220.168.19.65	255.255.255.255	1	1
169.254.0.0	255.255.0.0	65535	2

图 5-27 “子网统计”对话框

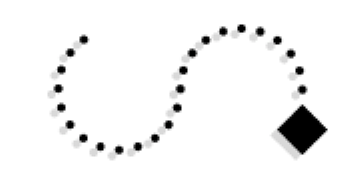


图 5-28 网段内的 IP 信息

捷菜单，进行 IP 定位、IP-MAC 绑定、端口连接设备统计等的操作，在下文中我们将详细阐述。

3. 网段统计

对全网中已用和未用的 IP 地址资源进行统计，提供参考依据。根据扫描结果，系统详细地统计出了已分配和未分配的 IP 地址、MAC 地址、设备名和设备类型等信息，对统计结果分别以列表和图形进行展示，如图 5-29 所示。



IP网段分配情况统计

标签含义

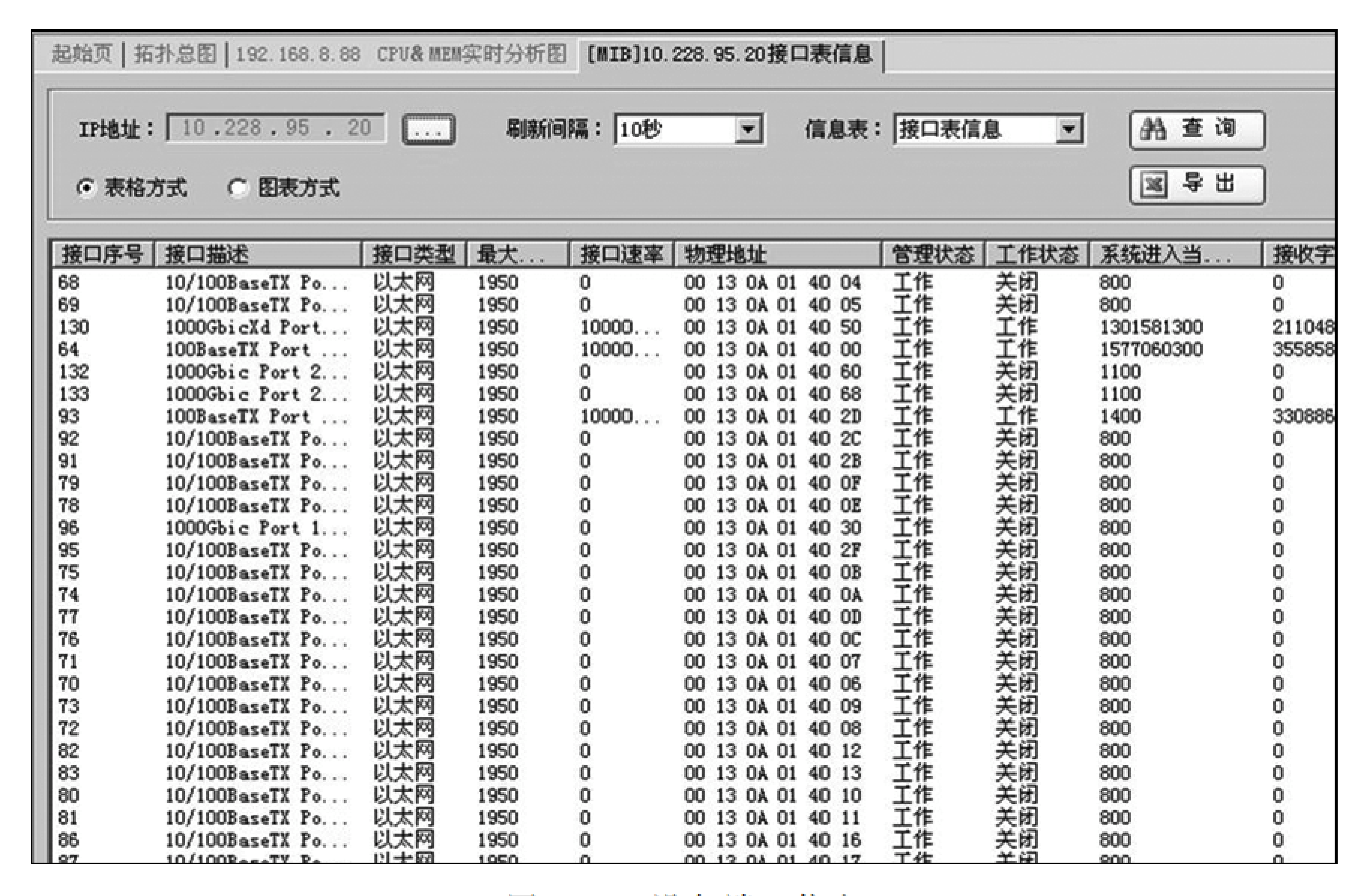
子网IP：10.8.0.0　　已分配　　未活动

10.8.0.1	10.8.0.2	10.8.0.3	10.8.0.4	10.8.0.5	10.8.0.6	10.8.0.7	10.8.0.8	10.8.0.9
10.8.0.10	10.8.0.11	10.8.0.12	10.8.0.13	10.8.0.14	10.8.0.15	10.8.0.16	10.8.0.17	10.8.0.18
10.8.0.19	10.8.0.20	10.8.0.21	10.8.0.22	10.8.0.23	10.8.0.24	10.8.0.25	10.8.0.26	10.8.0.27
10.8.0.28	10.8.0.29	10.8.0.30	10.8.0.31	10.8.0.32	10.8.0.33	10.8.0.34	10.8.0.35	10.8.0.36
10.8.0.37	10.8.0.38	10.8.0.39	10.8.0.40	10.8.0.41	10.8.0.42	10.8.0.43	10.8.0.44	10.8.0.45
10.8.0.46	10.8.0.47	10.8.0.48	10.8.0.49	10.8.0.50	10.8.0.51	10.8.0.52	10.8.0.53	10.8.0.54
10.8.0.55	10.8.0.56	10.8.0.57	10.8.0.58	10.8.0.59	10.8.0.60	10.8.0.61	10.8.0.62	10.8.0.63
10.8.0.64	10.8.0.65	10.8.0.66	10.8.0.67	10.8.0.68	10.8.0.69	10.8.0.70	10.8.0.71	10.8.0.72
10.8.0.73	10.8.0.74	10.8.0.75	10.8.0.76	10.8.0.77	10.8.0.78	10.8.0.79	10.8.0.80	10.8.0.81
10.8.0.82	10.8.0.83	10.8.0.84	10.8.0.85	10.8.0.86	10.8.0.87	10.8.0.88	10.8.0.89	10.8.0.90
10.8.0.91	10.8.0.92	10.8.0.93	10.8.0.94	10.8.0.95	10.8.0.96	10.8.0.97	10.8.0.98	10.8.0.99
10.8.0.100	10.8.0.101	10.8.0.102	10.8.0.103	10.8.0.104	10.8.0.105	10.8.0.106	10.8.0.107	10.8.0.108
10.8.0.109	10.8.0.110	10.8.0.111	10.8.0.112	10.8.0.113	10.8.0.114	10.8.0.115	10.8.0.116	10.8.0.117
10.8.0.118	10.8.0.119	10.8.0.120	10.8.0.121	10.8.0.122	10.8.0.123	10.8.0.124	10.8.0.125	10.8.0.126
10.8.0.127	10.8.0.128	10.8.0.129	10.8.0.130	10.8.0.131	10.8.0.132	10.8.0.133	10.8.0.134	10.8.0.135
10.8.0.136	10.8.0.137	10.8.0.138	10.8.0.139	10.8.0.140	10.8.0.141	10.8.0.142	10.8.0.143	10.8.0.144
10.8.0.145	10.8.0.146	10.8.0.147	10.8.0.148	10.8.0.149	10.8.0.150	10.8.0.151	10.8.0.152	10.8.0.153
10.8.0.154	10.8.0.155	10.8.0.156	10.8.0.157	10.8.0.158	10.8.0.159	10.8.0.160	10.8.0.161	10.8.0.162

图 5-29　IP 网段分配情况统计

4. 端口连接设备统计

此功能供用户查看和统计当前设备与其他设备的连接状态。设备端口信息包括 IP 地址、MAC 地址、端口描述、连接设备、连接端口描述、连接设备类型、端口管理状态、端口连接状态，如图 5-30 所示。在图中可见，窗口的状态栏中，系统详细列出了当前设备所连接的其他设备的数据统计。



起始页 | 拓扑总图 | 192.168.8.88 CPU& MEM实时分析图 | [MIB]10.228.95.20接口表信息

IP地址：10.228.95.20　刷新间隔：10秒　信息表：接口表信息　查询　导出

表格方式　图表方式

接口序号	接口描述	接口类型	最大...	接口速率	物理地址	管理状态	工作状态	系统进入当...	接收字
68	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 04	工作	关闭	800	0
69	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 05	工作	关闭	800	0
130	1000GbicXd Port...	以太网	1950	10000...	00 13 0A 01 40 50	工作	工作	1301581300	211048
64	100BaseTX Port ...	以太网	1950	10000...	00 13 0A 01 40 00	工作	工作	1577060300	355858
132	1000Gbic Port 2...	以太网	1950	0	00 13 0A 01 40 60	工作	关闭	1100	0
133	1000Gbic Port 2...	以太网	1950	0	00 13 0A 01 40 68	工作	关闭	1100	0
93	100BaseTX Port ...	以太网	1950	10000...	00 13 0A 01 40 2D	工作	工作	1400	330886
92	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 2C	工作	关闭	800	0
91	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 2B	工作	关闭	800	0
79	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 0F	工作	关闭	800	0
78	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 0E	工作	关闭	800	0
96	1000Gbic Port 1...	以太网	1950	0	00 13 0A 01 40 30	工作	关闭	800	0
95	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 2F	工作	关闭	800	0
75	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 0B	工作	关闭	800	0
74	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 0A	工作	关闭	800	0
77	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 0D	工作	关闭	800	0
76	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 0C	工作	关闭	800	0
71	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 07	工作	关闭	800	0
70	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 06	工作	关闭	800	0
73	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 09	工作	关闭	800	0
72	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 08	工作	关闭	800	0
82	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 12	工作	关闭	800	0
83	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 13	工作	关闭	800	0
80	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 10	工作	关闭	800	0
81	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 11	工作	关闭	800	0
86	10/100BaseTX Po...	以太网	1950	0	00 13 0A 01 40 16	工作	关闭	800	0

图 5-30　设备端口信息

5.5.2 IP-MAC 基准数据

此模块相当于一个参照物，用户可以导入最原始的IP-MAC数据，来作为最准确的IP-MAC数据，并以此为基准，探测网内有没有违规IP地址行为；它为IP-MAC绑定提供标准的数据，为IP-MAC异动提供参考的依据。用户添加/删除网络设备、添加/删除线路，修改IP地址等诸如此类的操作之后，系统会自动更新IP-MAC数据，用户可以随时重新导入最新的IP-MAC数据。

单击“IP资源管理”→“IP-MAC基准数据”，单击菜单项，或者打开快捷菜单，可进行相关操作。

1. IP-MAC 导入

第一次使用程序的时候，用户必须先导入IP-MAC数据，单击IP-MAC导入，打开如图5-31所示的对话框。



图5-31 IP-MAC导入数据

单击“刷新”可以得到最新的IP-MAC数据。在对话框中勾选需要导入的数据，也可以选择全部，单击“保存”，系统提示导入数据成功，并将数据列在IP-MAC基准数据的结果窗口中，如图5-32所示。

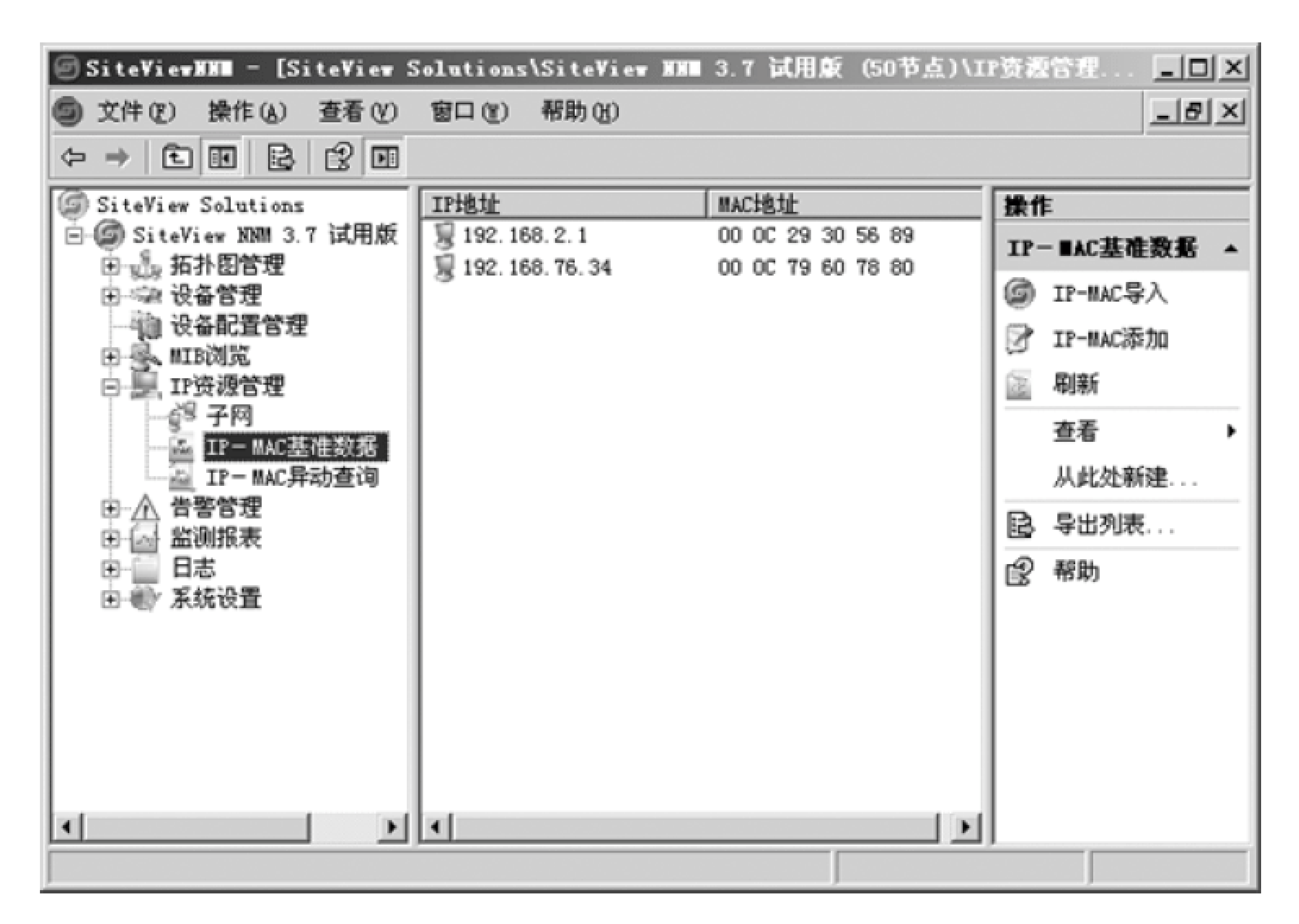
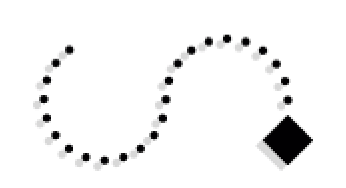


图5-32 IP-MAC导入结果

2. IP-MAC 添加

系统提供了手工添加IP-MAC数据的功能，单击“IP-MAC添加”，如图5-33所示。



必须输入正确的格式，否则无法保存。输入完成后，单击“添加”，系统提示添加成功即可。

3. 删除

即删除 IP-MAC 地址列表中的一条或者多条记录，删除后如需重新添加，可以通过 IP-MAC 导入实现。

4. 编辑

即设备 IP、MAC 地址的修改，在 IP-MAC 地址列表中选中需要修改的记录，单击“编辑”，打开如图 5-34 所示的窗口。必须输入正确的格式，否则无法保存。



图 5-33　添加 IP-MAC 数据



图 5-34　IP-MAC 修改

5.5.3　IP-MAC 异动查询

以 IP-MAC 数据修改模块中的数据为基准，系统探测到 IP 地址和 MAC 地址做过修改，自动将数据搜集，以供用户查询和分析，更好地监控管理 IP 资源。当网内 IP 地址发生冲突时，用户可以在此窗口中查询到该 IP 地址被哪些 MAC 地址占用过。单击“IP 资源管理”→“IP-MAC 异动查询”，打开如图 5-35 所示的窗口。

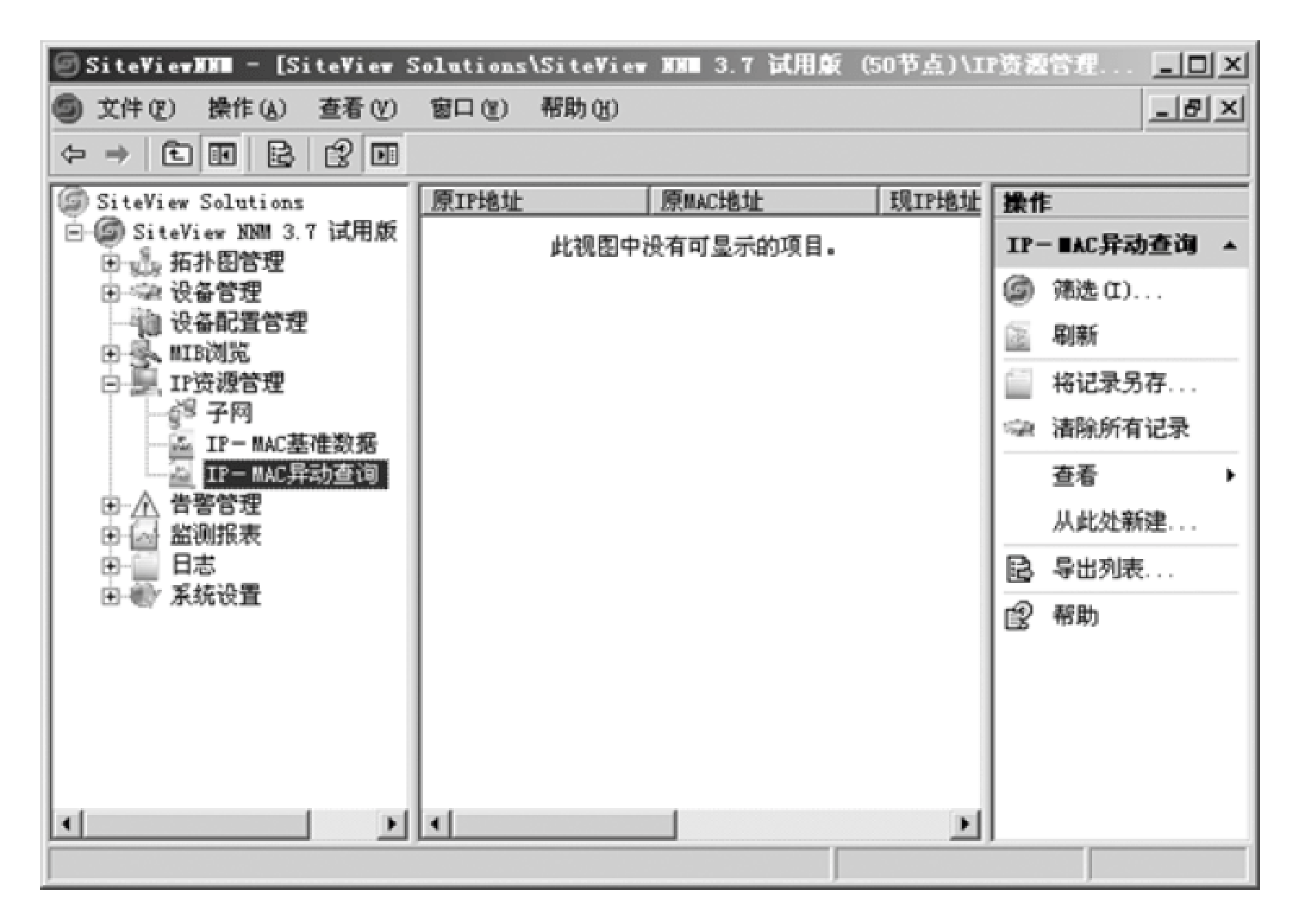


图 5-35　IP-MAC 异动数据查询



图 5-36　查询筛选器

数据比较多的时候，在图 5-35 中进行查找和统计比较麻烦，系统提供了筛选的功能，用户可自定义过滤条件，如图 5-36 所示。

输入 IP 地址和 MAC 地址，也可以只单独输入其中一个，选择起始终止日期和需要显示的记录数限制，系统提供了 10，50，100，200，500，1000 这 6 种选择，单击“确定”，系统即统计出过滤条件所有的变动记录及被系统监测到的时间。如想返回查看所有 IP、MAC 地址的异动记录，则在此窗口中不输入 IP 地址和 MAC 地址，只选择记录数限制和起止日期即可。

5.6　SiteView NNM 告警管理

告警管理相当于一个预警的模块，用来控制设备的使用情况不超出我们网络环境承受的范围，同时即时提出告警，以使其不产生无法控制的局面。它可以设置设备的告警模式，通过语音、邮件、手机短信等载体传达告警内容，从而达到对设备进行实时监控的目的。它由告警方式、告警设置、告警记录三部分组成。

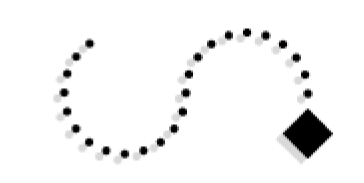
5.6.1　告警方式

告警方式即设置告警策略、告警的通知方法和需要通知的对象，主要的通知方式有：软件界面、语音、邮件、手机短信。单击“告警管理”→“告警方式”→“新建策略”，打开“告警方式”窗口，如图 5-37 所示。



图 5-37　“告警方式”窗口

软件界面告警是系统默认的告警方式，它将系统产生的告警数据通过拓扑图管理模块，用设备告警标注和线路变换颜色的方式通知用户。对于其他警告形式，这里以邮箱告



警策略的设定来说明。在图 5-37 中，输入策略名称，如 interface，选择“是否语音告警”，单击“新增”，打开“Email(短信)设置”对话框，如图 5-38 所示，根据提示输入相关信息，单击“保存”退出即可。



图 5-38　“Email(短信)设置”对话框

5.6.2　告警设置

告警设置用于设置设备的告警阈值、告警策略、设备信息采集频率、告警延迟次数等信息。系统一共提供了 18 个监视项目供用户进行网络监控，它们分别为：IP-MAC 绑定、Ping 检测、SNMPPing 检测、CPU 负载、内存占用、总流量、入流量、出流量、总帧流量、入帧流量、出帧流量、总丢包率、发送丢包率，接收丢包率，总错包率、发送错包率、接收错包率、总广播包，如图 5-39 所示。

每个监视项目都附有说明，用户可根据自身需要分别进行设置。除 IP-MAC 绑定作为一种特殊的分类方法之外，其余 17 个监视项目均可以通过按设备分类、按指标分类、快捷方式来设置，故这里重点介绍这 4 种分类方法。可以一个项目一个项目地设置告警，也可以使用其中一种分类方法将 18 个项目全部设置完成，这里以按设备分类、IP-MAC 绑定来说明。

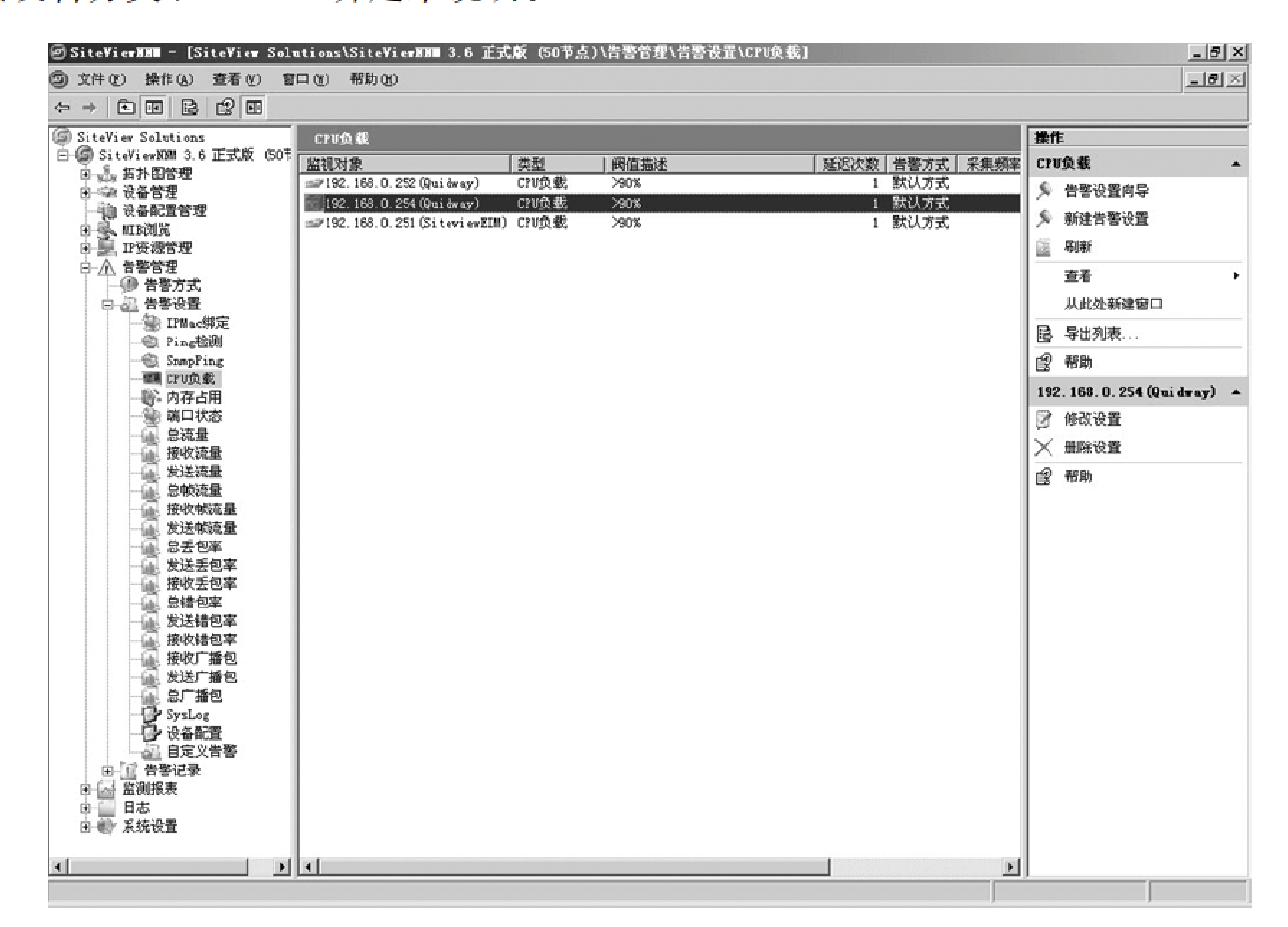


图 5-39　告警设置内容

1. 按设备分类

单击“告警管理”→“告警设置”→“监视项目”→“总流量”→“新建告警设置”命令，打开“告警设置”窗口，如图 5-40 所示。

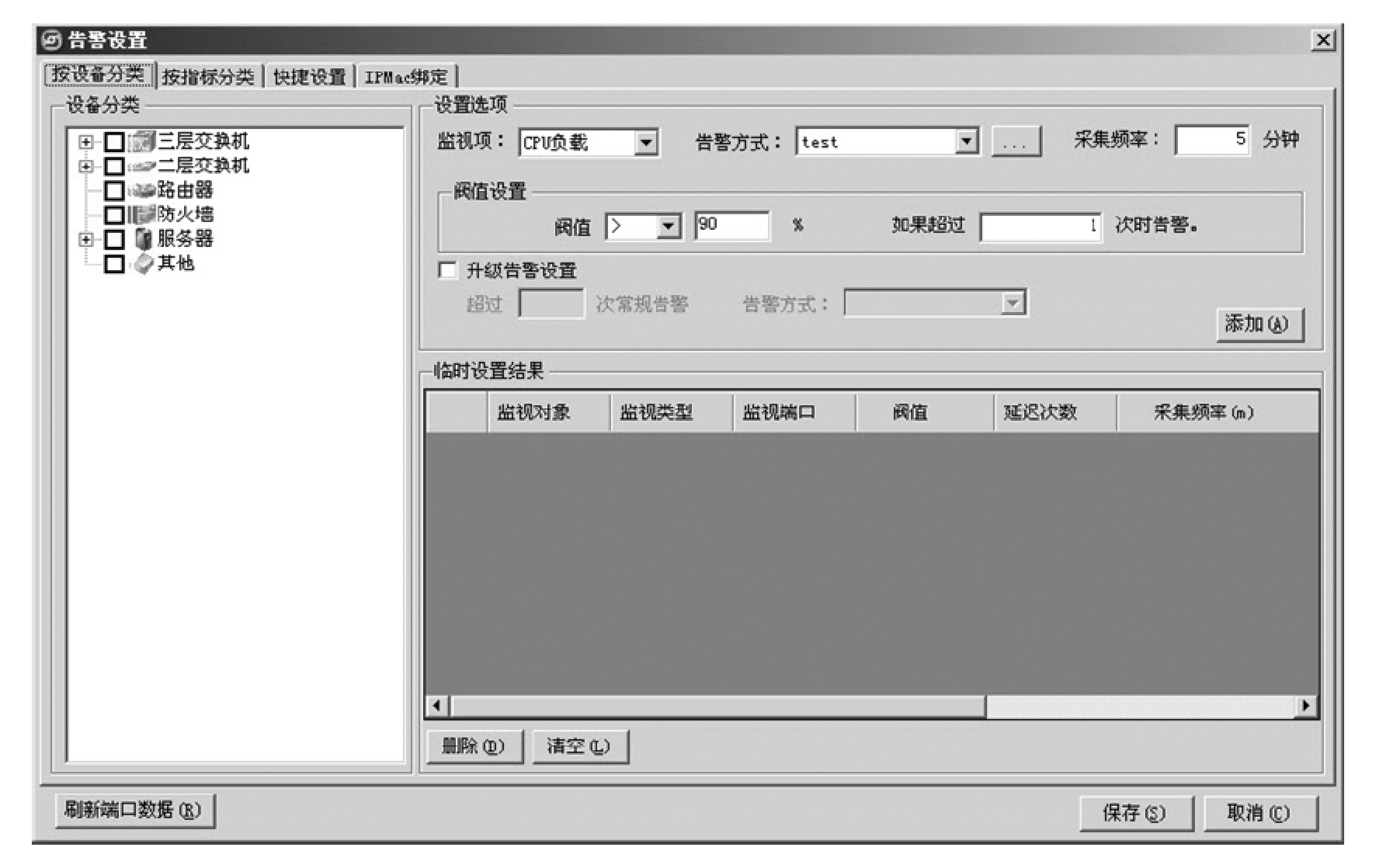


图 5-40 “告警设置”窗口

窗口的设备分类树中,列出了网内所有设备的 IP 地址,这些数据是从设备管理模块中取到的,随设备管理的数据更改而更新。

监视项:“监视项”下拉框中,列出了除 IP-MAC 绑定之外的 17 个项目。

设备分类:可以全选,也可以一一勾选。

指定端口:当对三层交换机、二层交换机、路由器、服务器这些设备进行总流量、入流量、出流量、总帧流量、入帧流量、出帧流量、总丢包率、发送丢包率、接收丢包率、总错包率、发送错包率、接收错包率、总广播包进行监视时,指定端口的下拉框才能进行选择。

刷新端口数据:在指定端口之前,必须先得到最新的设备端口数据,单击“刷新端口数据”可以实现。端口的刷新可以按设备、子网和 IP 地址列表三种方式进行,选择需要刷新的设备,如图 5-41 所示,单击“确定”即可。



图 5-41 选择设备

告警方式:单击下拉框进行选择,单击[...],系统返回新建告警方式窗口,用户可添加新的告警方式。

采集频率:以分钟为单位,用户可自定义每过多少分钟采集一次告警数据并通知用户。

阈值:设置告警的阈值条件,用户可视网络环境自定义。

“添加”:每定义完一个监视项目的告警,单击“添加”,系统就将数据添加到临时设备结果框中;用户可以把所有的监视项目全部设置告警;也可以对同一监视项目指定不同的告警方式,搭配不同的阈值;总而言之,可以组成任意一个搭配一一添加。

“删除/全部删除”:对临时设置结果的数据实现单个删除和全部删除。

设置完成后,单击“保存”退出即可。

2. IP-MAC 绑定

由于需要实现对违规 IP 地址行为的监控和自动有效的处理，并与 IP 资源管理模块相结合，共享数据，系统将 IP-MAC 绑定单独作为一个告警设置项目，如图 5-42 所示。



图 5-42　IP-MAC 绑定的告警设置

(1) 若要添加绑定项，则单击"添加绑定项"，打开窗口，如图 5-43 所示。

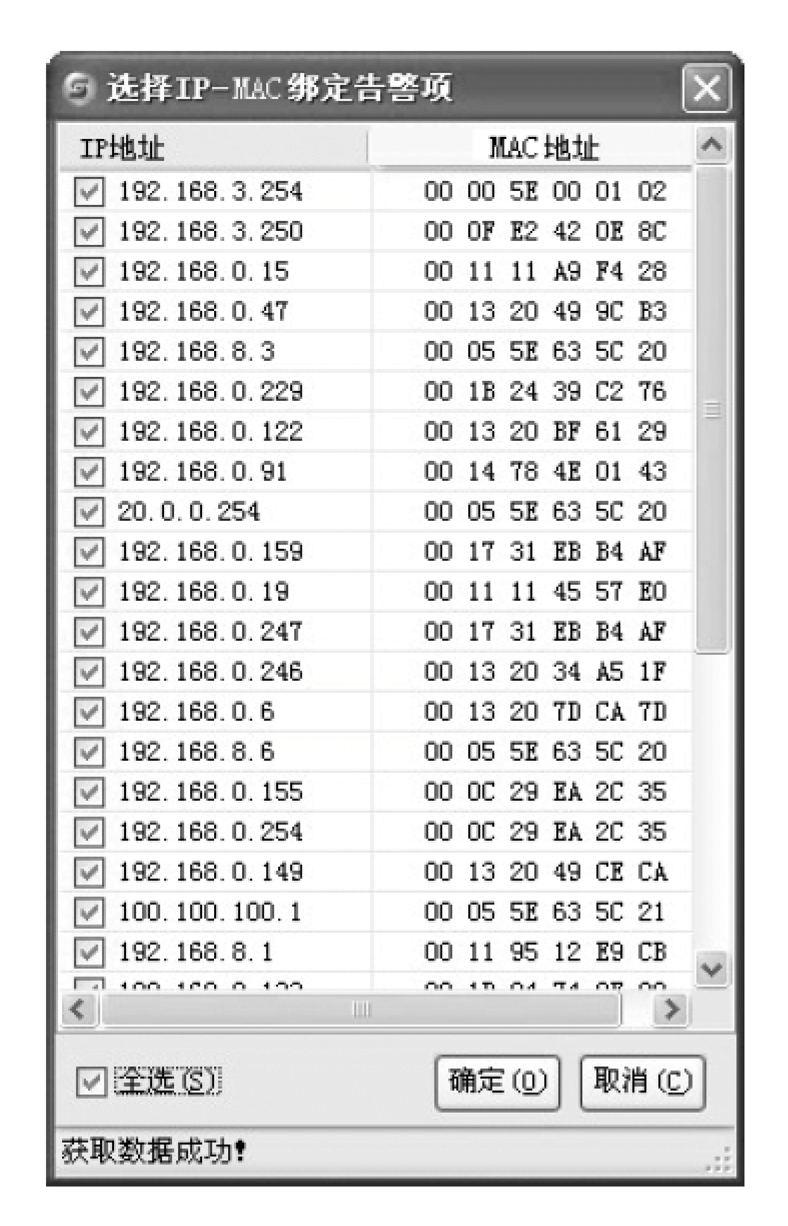


图 5-43　选择 IP-MAC 绑定

勾选 IP-MAC 地址，也可以单击"全选"，单击"确定"即添加成功。此窗口的数据和

IP-MAC 基准数据模块中的数据是共享的、同步的。所以，执行这个操作之前，必须先在 IP-MAC 基准数据模块中导入数据方可。

（2）在图 5-42 中，选择一条 IP 地址，单击“删除”可以实现删除。输入告警方式、采集频率，单击“保存”即可实现 IP-MAC 绑定告警设置。

5.6.3 告警记录

对已产生的历史告警和当前告警进行全面详细的记录，以供查询和备份，它支持查询设备告警的当前记录和历史记录。

1. 当前告警

和告警设置一样，当前告警也分成 18 个监视项目，与告警设置一一相对应。从告警设置成功时开始，系统记录了 100 条实时告警的详细信息，包括告警类型、关联设备、发生时间、告警描述，每隔 15 秒刷新一次，提取到最新的告警信息。

单击“告警管理”→“告警记录”→“当前告警”→“监视项目”命令，以总流量为例，如图 5-44 所示。

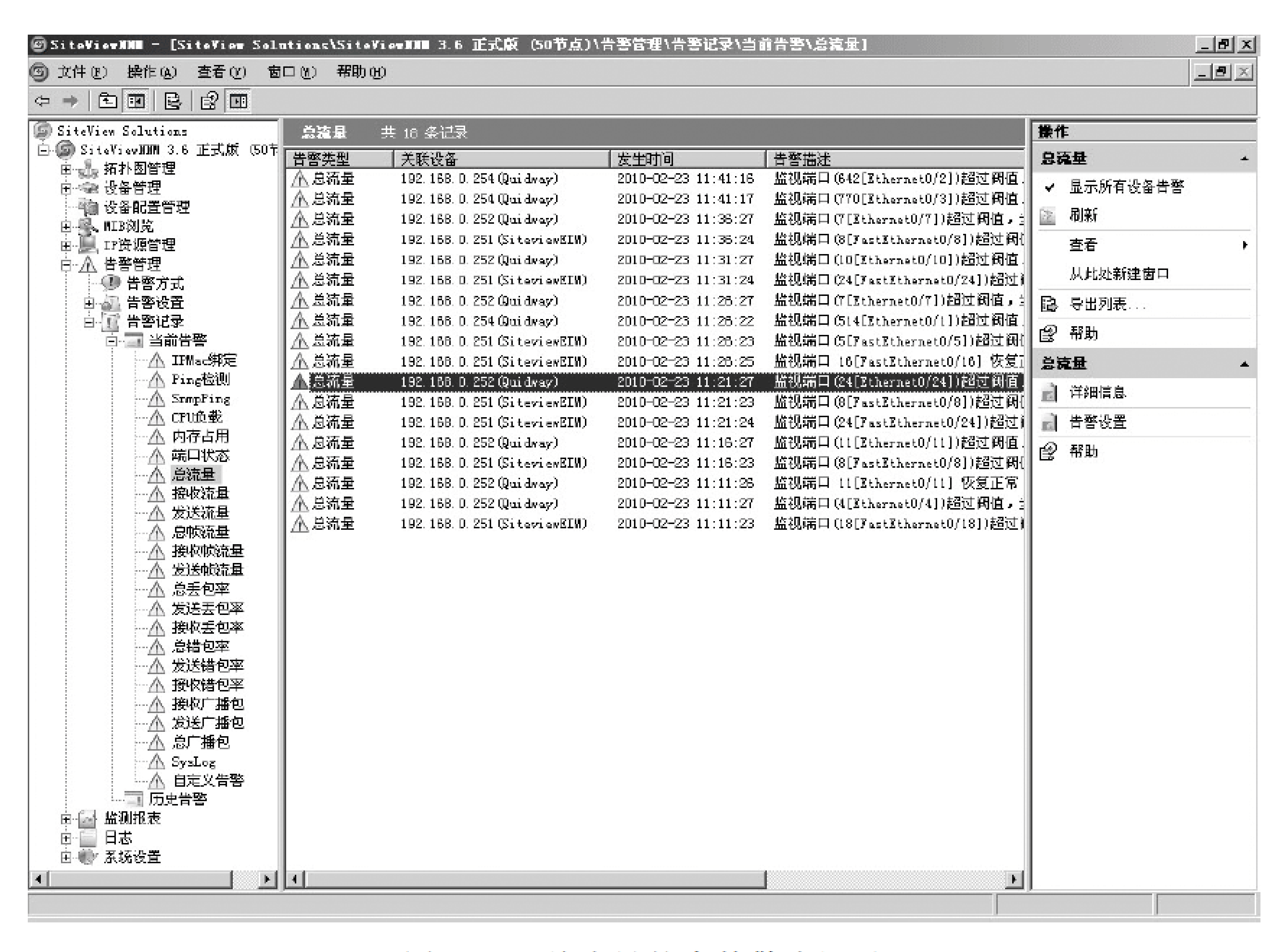
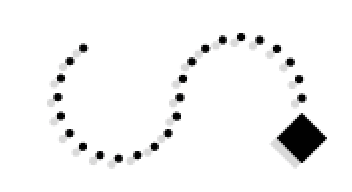


图 5-44 总流量的当前警告记录

2. 历史告警

系统对所有的告警数据作了全盘记录，并提供导出功能，支持用户进行统计分析和备份。单击“告警管理”→“告警记录”→“历史告警”命令，将展示全部历史警告，如图 5-45 所示。历史告警数据的保存期限与系统设置有关，最长可以保存 5 年，默认为保存 3 天。用户需要更改保存期限，必须先到系统设置模块进行历史数据管理设置。

单击右侧操作栏的“查询”按钮，通过选择起始时间、结束时间、监视项目、监视设备等信息，如图 5-46 所示，系统将符合查询条件的数据在查询结果对话框中罗列出来。



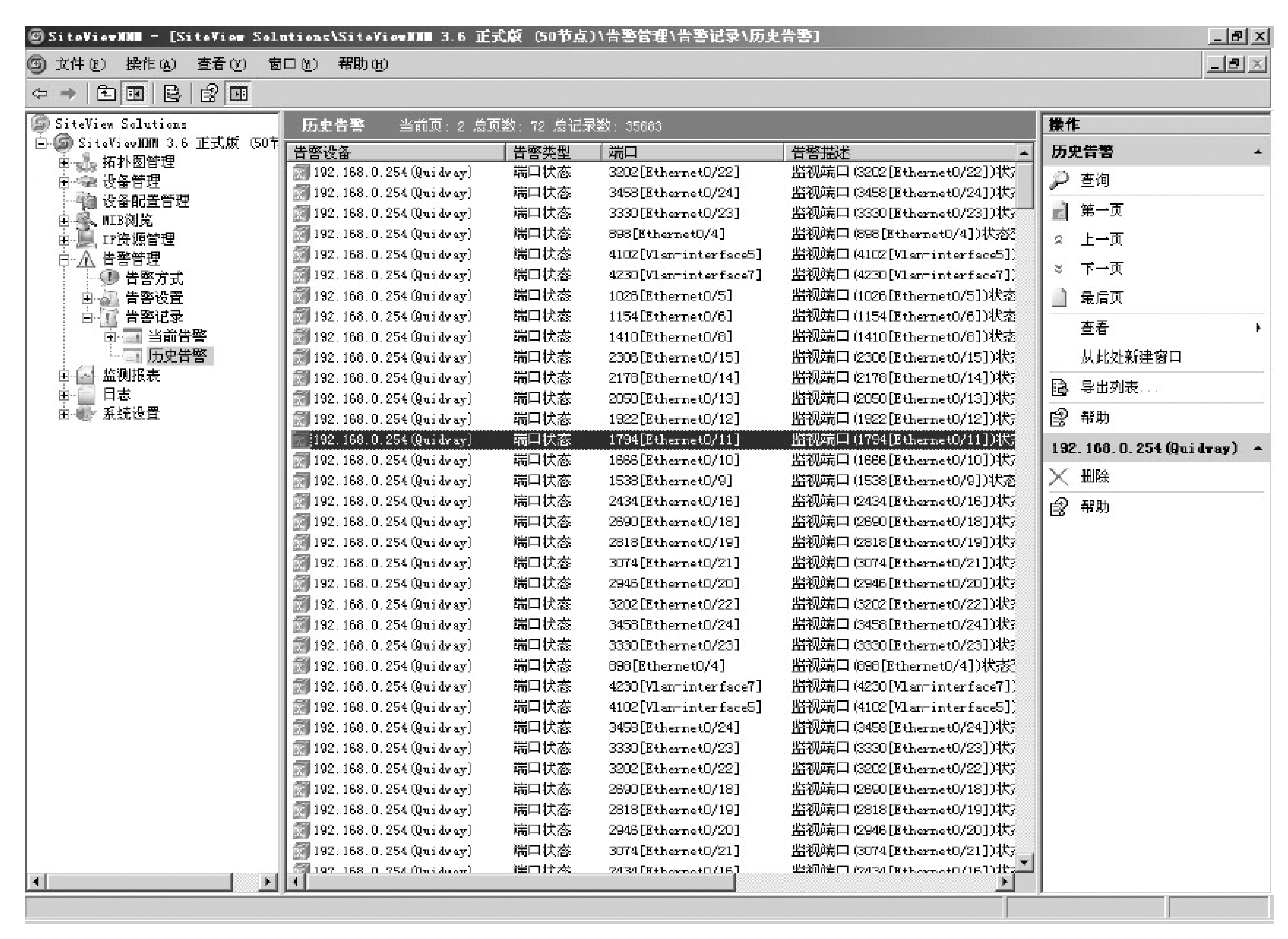


图 5-45　历史警告记录



图 5-46　历史记录查询条件设置

5.7　SiteView NNM 监测报表

监测报表模块全盘记录了网络情况，可进行相关的统计分析；提供多种灵活的查询条件生成各式报表输出，并提供了直观简明的图表报告，还可导出成 Excel 等文件格式，方便打印和保存。

为节约查询时间，在不退出 SiteView NNM 的情况下，报表的查询结果都不会随操

作模块的更改而丢失。比如由正在查询的报表模块转移到告警模块执行了相关操作，再返回该报表后，可以看见，之前查询的结果仍在。

5.7.1 设备端口状态实时分析

它可以对设备的端口、CPU、内存使用率、链路的通断、流量等实时信息和运行状态全盘记录，并输出成直观简明的图表和 Excel 文档。设备端口状态实时分析包括设备端口状态实时分析和 CPU&MEM 实时分析两部分内容。

1. 设备端口状态实时分析

单击“监测报表”→“设备端口状态实时分析”→“设备端口状态实时分析”命令。

它可以读取可网管设备的端口相关信息、流量值，并提供对单个端口的流量状况图形分析，对所有端口进行流量分析对比。这里以端口分析、多端口对比分析为例说明。

(1) 端口分析

图 5-47 中，在端口列表中，双击选择处于工作状态中的端口，系统给出了当前查询端口的文字信息，以图表的方式列出了该端口的各流量值，包括总流量、发送接收流量、出入帧流量、出入广播量。

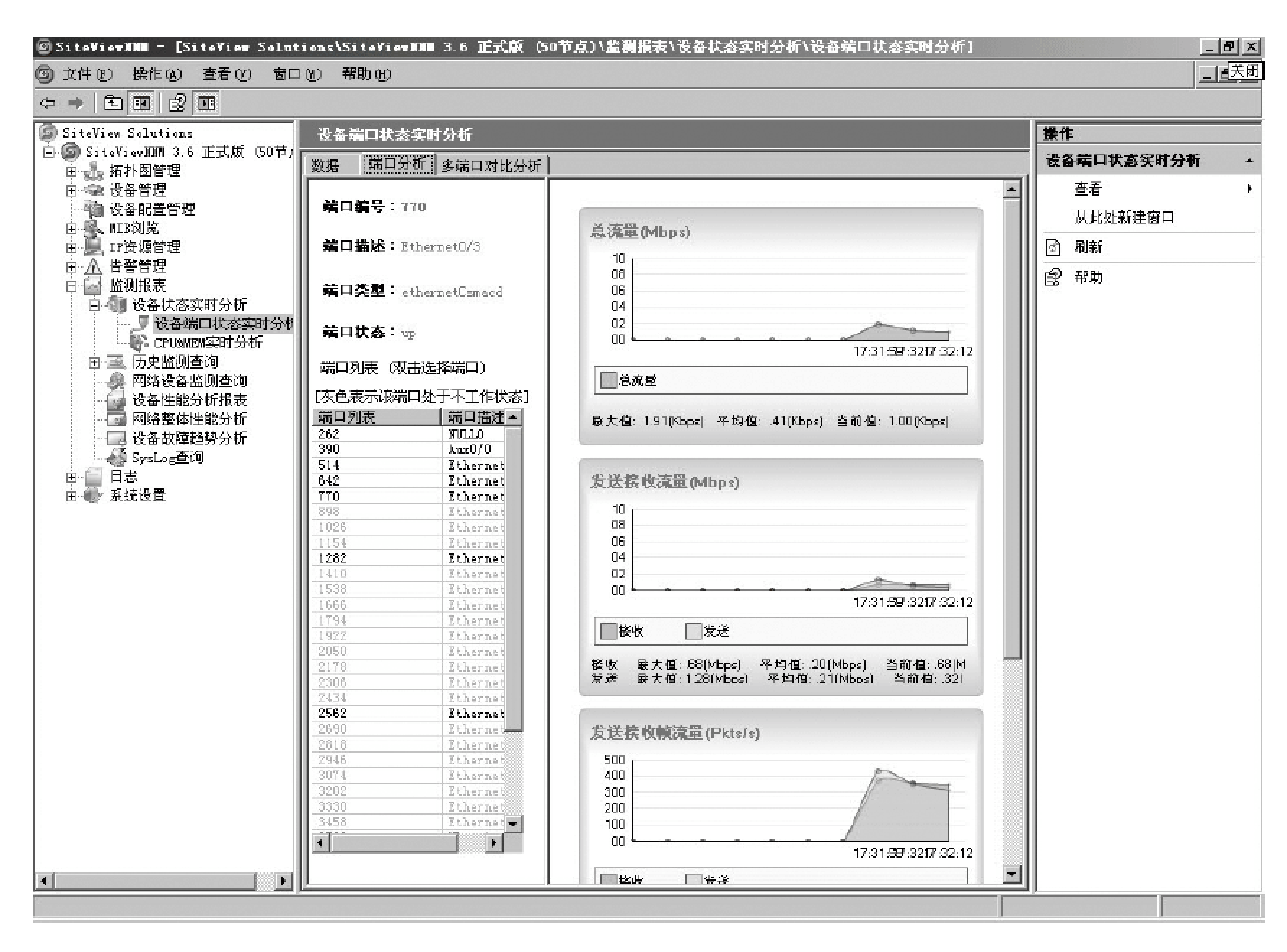


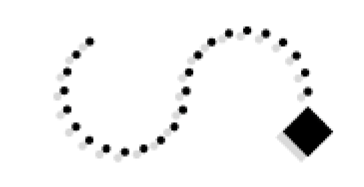
图 5-47 端口分析

(2) 多端口对比分析

以流量为基准，取多个端口的同一个流量进行对比和分析。如图 5-48 所示，在“对比分析项”下拉框中选择监测项目，在端口列表中选择处于工作状态中的端口，每增加一个端口就自动增加一张图表。

2. CPU&MEM 实时分析

单击“监测报表”→“设备端口状态实时分析”→“CPU&MEM 实时分析”命令。



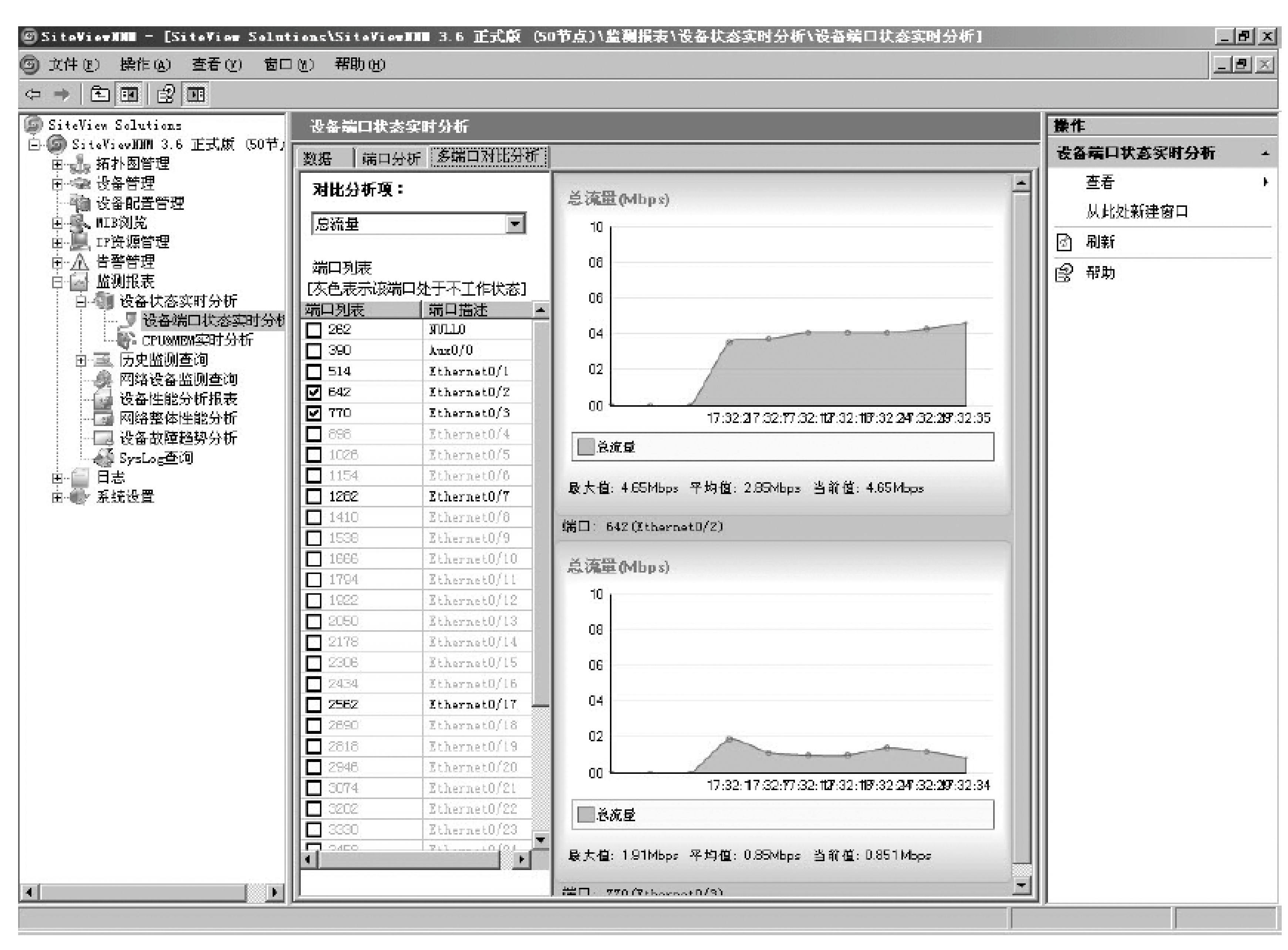


图 5-48　多端口对比分析

它可以查看和分析可网管设备的实时 CPU 利用率以及内存占用率，以图文结合的方式表现出来，并随时刷新读取最新的数据。如图 5-49 所示，选择刷新时间间隔，单击[...]选择设备地址，系统自动开始监测，并且一直处于监测的状态，直到用户单击“停止”按钮为止。

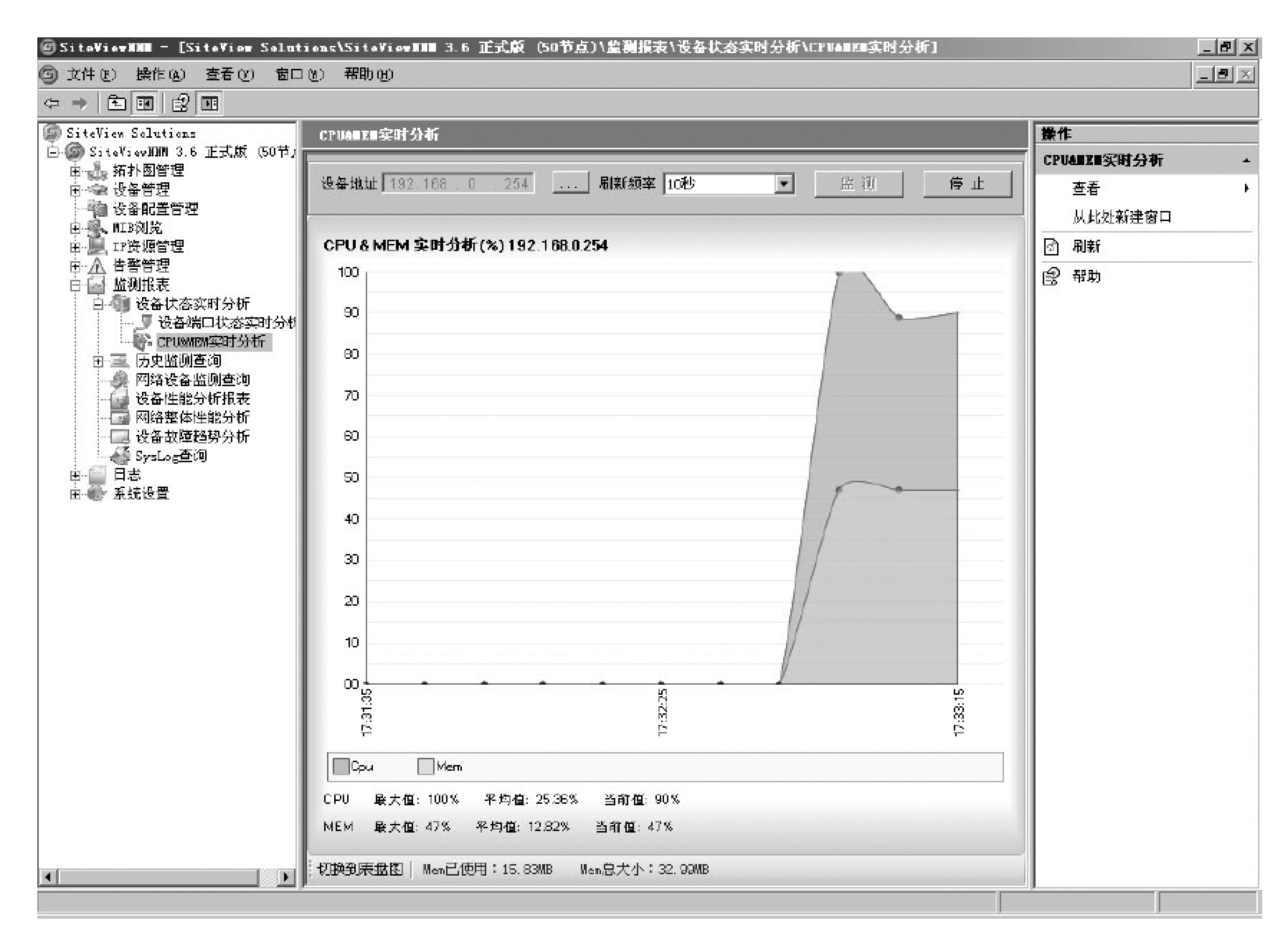


图 5-49　CPU&MEM 实时分析

除折线图之外，系统还列出了当前设备 CPU&MEM 的最大值、平均值、当前值以及 MEM 总大小和已使用的数值。单击“切换到罗盘图”，用户可以使用一种更易理解、更为真实的方式查看。

5.7.2 历史监测查询

历史监测查询能够根据用户的需要对设备端口、CPU、内存等的数据、流量及性能指标进行历史数据采集，体现其变化规律，并根据分类予以统计分析。

1. 端口历史数据查询

单击“监测报表”→“历史监测查询”→“端口历史数据查询”命令，如图 5-50 所示。与设备端口状态实时分析相对应，它采集的是设备端口的历史流量数据。系统把历史流量数据分成五个监测类型组，作为查询条件之一，分别是：发送/接收流量、出帧/入帧流量、发送/接收丢包率、发送/接收错包率、总流量/总帧流量；以设定的查询时间为基准，可查询本日、本周、本月的历史数据。所有的查询条件设定好之后，单击“查询”即可，如需保存电子版本，可单击“导出”实现。

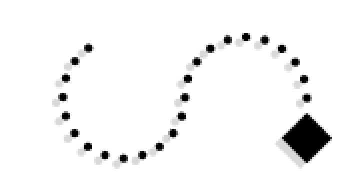


图 5-50 端口历史数据查询

2. CPU&MEM 历史数据查询

单击“监测报表”→“历史监测查询”→“CPU&MEM 历史数据查询”命令。

如图 5-51 所示，与 CPU&MEM 实时分析相对应，它采集的是 CPU&MEM 的历史监测数据，用表格和图表两种方式形象直观的输出，以设定的查询时间为基准，可查询本日、本周、本月的历史数据。所有的查询条件设定好之后，单击“查询”即可，如需保存电子版本，在表格方式中，可单击“导出”得以实现。



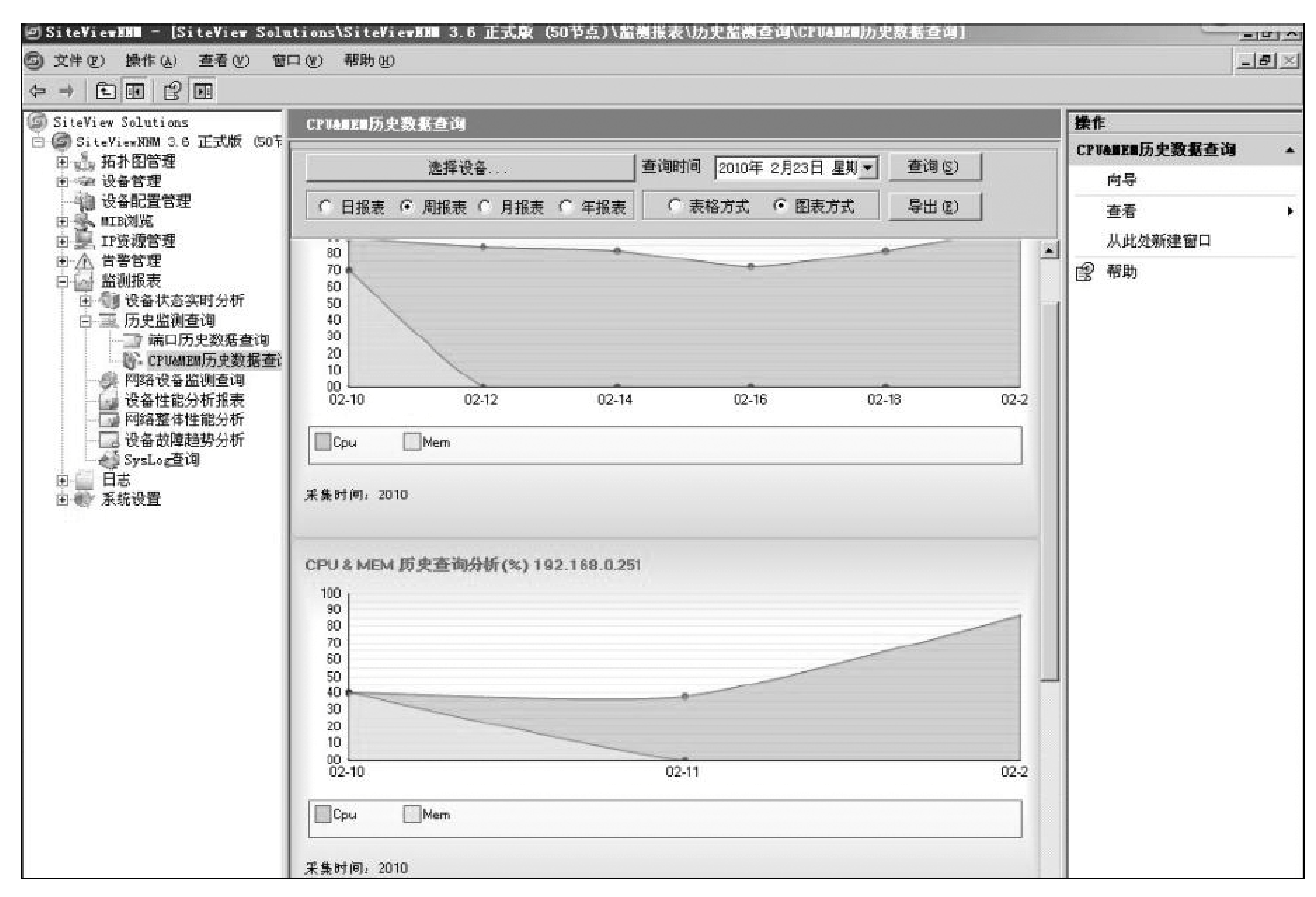


图 5-51　CPU&MEM 历史数据查询

5.7.3　网络设备监测查询

它可以监测设备的端口流量值、设备运行的状况和性能数据。查询结果之前，用户必须先设定查询的条件。单击“监测报表”→“网络设备监测查询”命令，出现如图 5-52 所示界面，它还提供查询结果的图形显示方式，如图 5-53 所示。

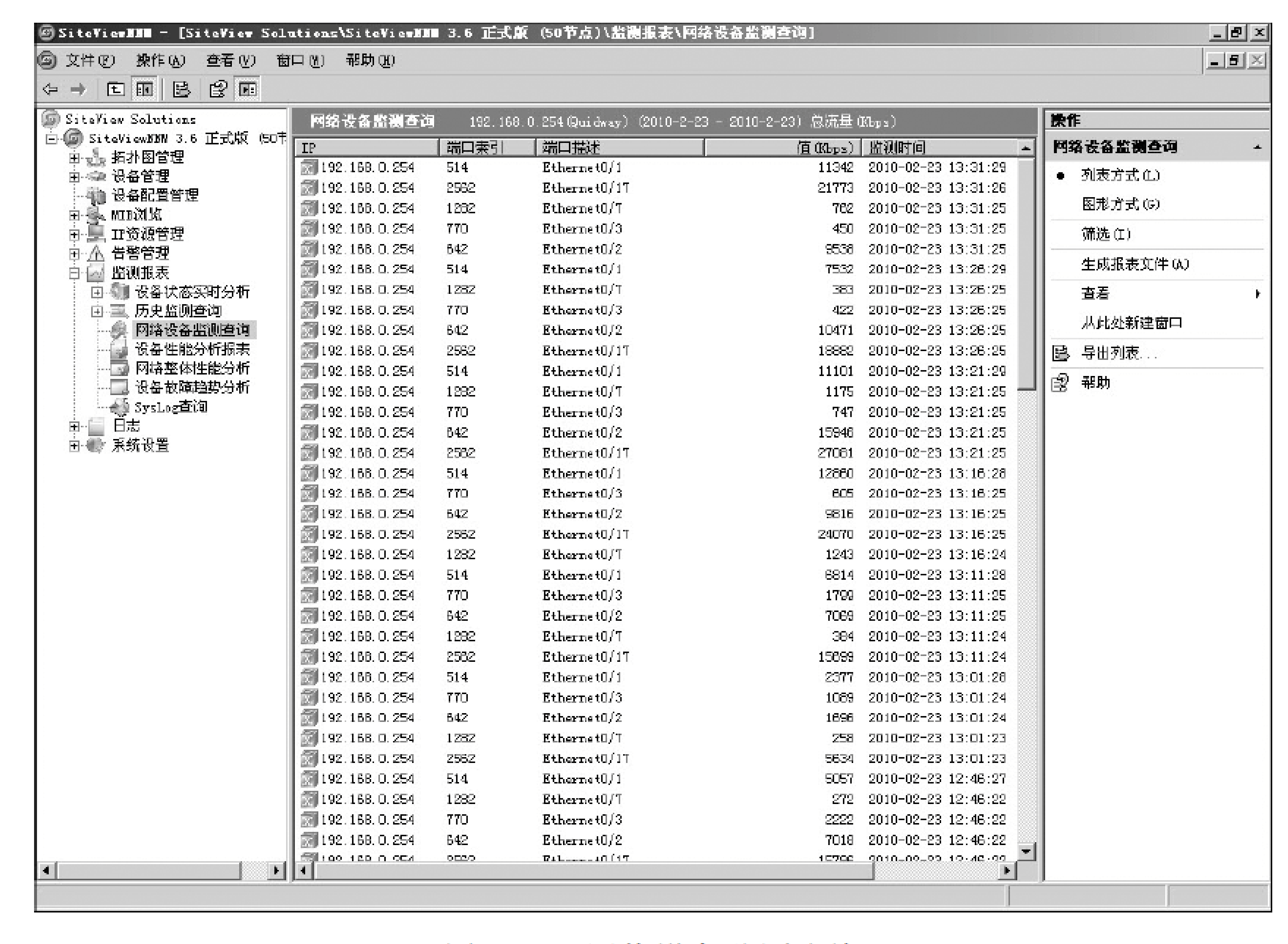


图 5-52　网络设备监测查询

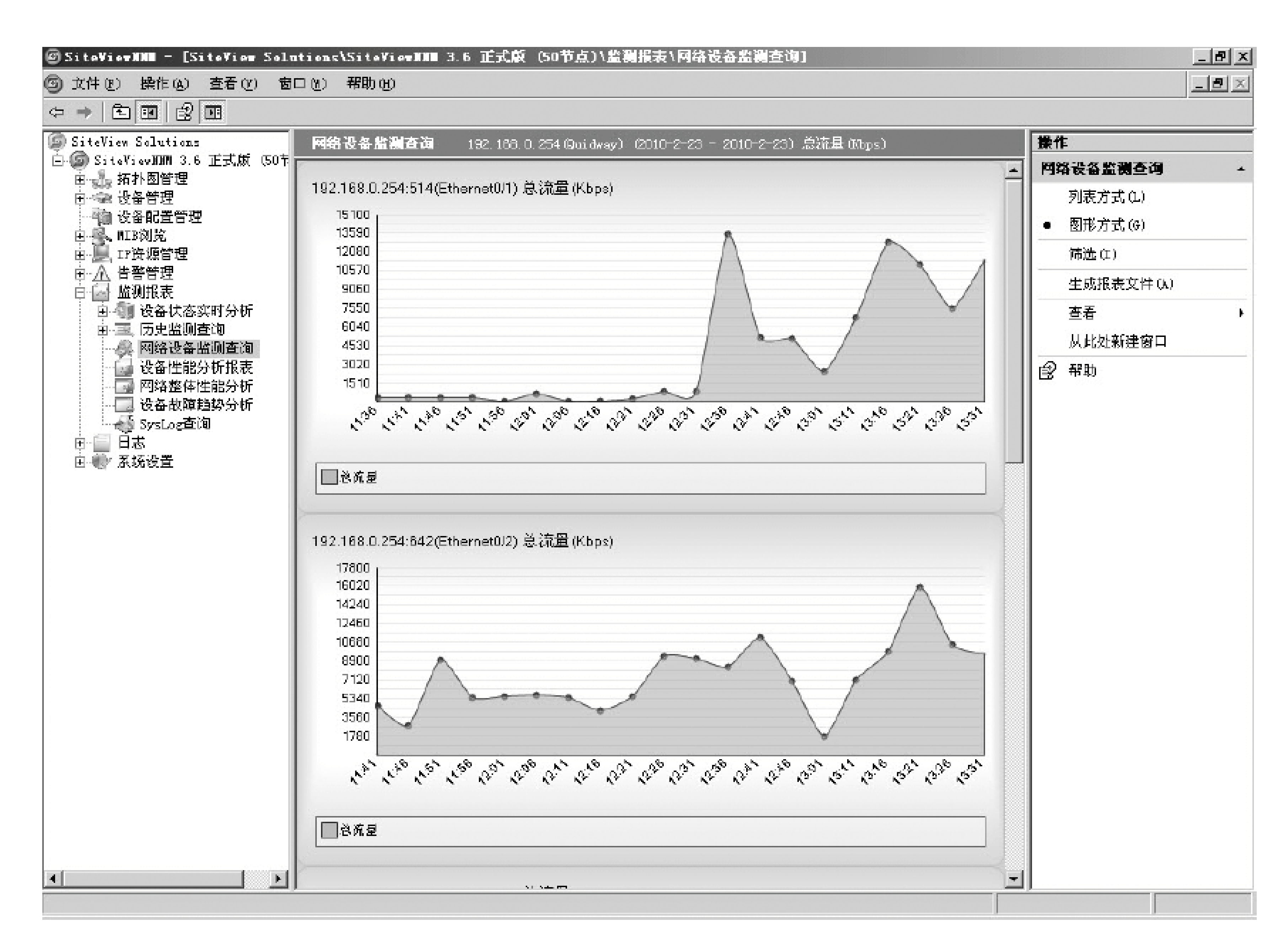


图 5-53　网络设备监测查询图形显示方式

在操作栏单击“筛选”按钮，打开筛选器，如图 5-54 界面。通过查询参数的设定，即可查询具体设备监测报表。



图 5-54　查询筛选器

5.7.4　设备性能分析报表

它主要提供对某段时间内网内设备各端口流量和性能的查询、统计，用户可以查看到这些数据的最大值和平均值。查询结果之前，用户必须先设定查询条件，单击“监测报表”→“设备性能分析报表”→“筛选”命令，打开筛选器，如图 5-55 所示。

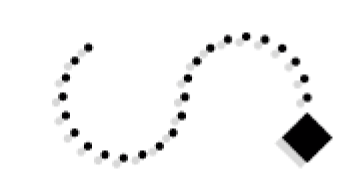




图 5-55　筛选器(1)

系统罗列了 19 个监测项目。在这些报表字段中,除“节点名称”和“设备中文名称”之外,选择“CPU 负载”和“内存占用”,其他的会变成灰色,不可选,反之亦然;“设备 IP”、“端口号”、“端口描述”是系统默认的报表字段,在这个窗口中没有列出来,表格生成后,会自动显示在报表中。

报表字段设定好之后,单击“确定”按钮,返回到设备性能分析报表的结果窗口中,选择设备、起始和结束的时间、报表格式,单击“查询”,系统输出报表,如图 5-56 所示,用户可单击“导出”,另存为 Excel 文档。

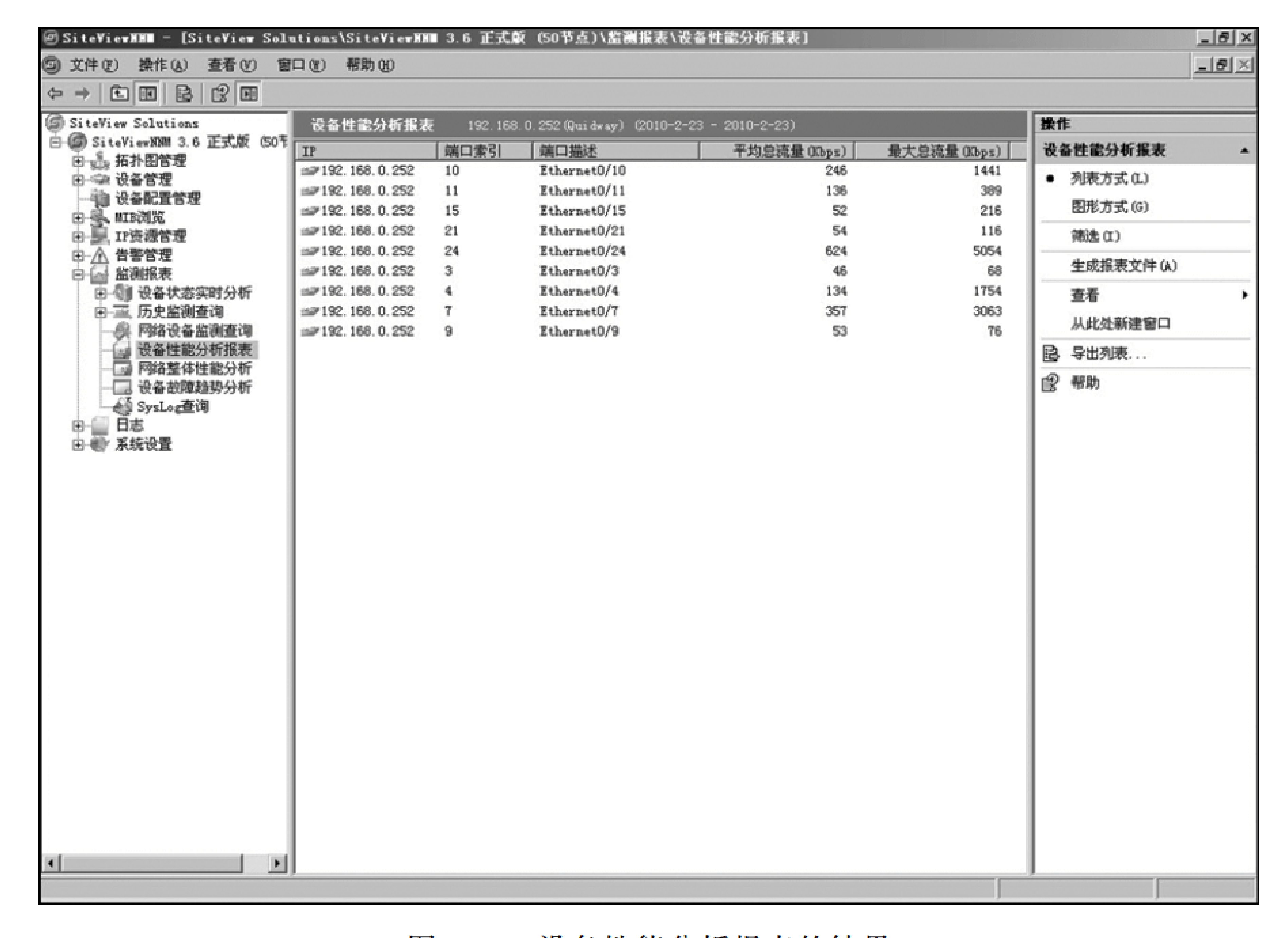
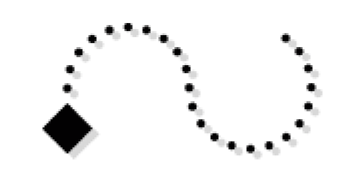


图 5-56　设备性能分析报表的结果



在图 5-56 中，单击“图形方式”，系统可将查询结果输出成图形，如图 5-57 所示。

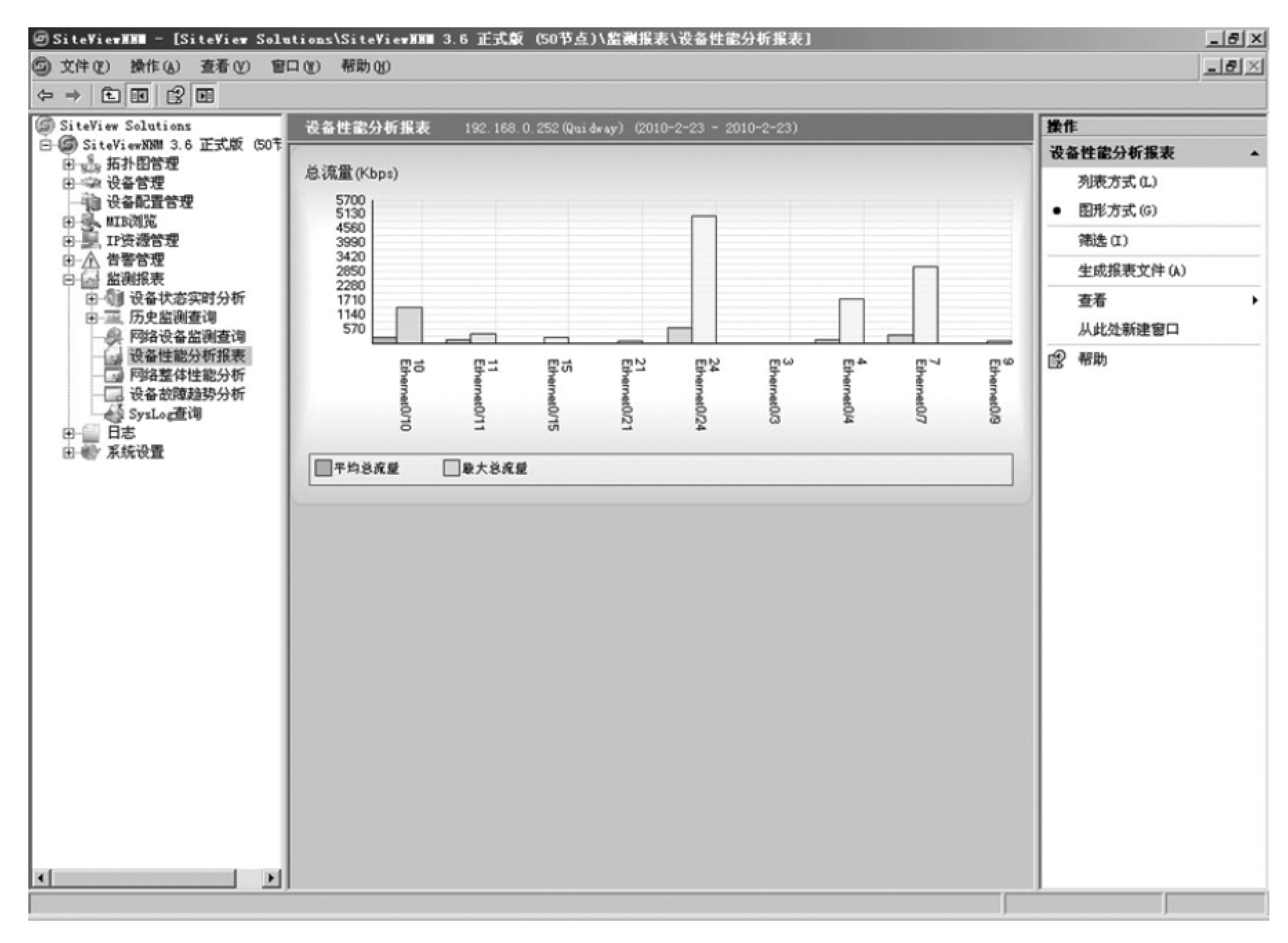


图 5-57　设备性能分析报表的结果图

5.7.5　网络整体性能分析

它可实现对网内所有设备的性能进行查询和统计。在报表中，用户可以查看到某时间段内，网内所有设备的所有端口，其监测项目的最大值和平均值，可选多个监测项目同时查询，用户可以据此进行网内设备性能分析。查询结果之前，必须先设定查询条件，单击“监测报表”→“网络整体性能分析”→“筛选”命令，打开筛选器，如图 5-58 所示。

系统提供了 12 个监测项目，可多选；但选择“内存占用”和“CPU 负荷”时，其他的监测项目会变成灰色，不可选，反之亦然；选择起始和结束时间之后，单击“确定”按钮，系统输出监测报表，如图 5-59 所示，用户可单击生成报表文件另存为 Excel 文档。

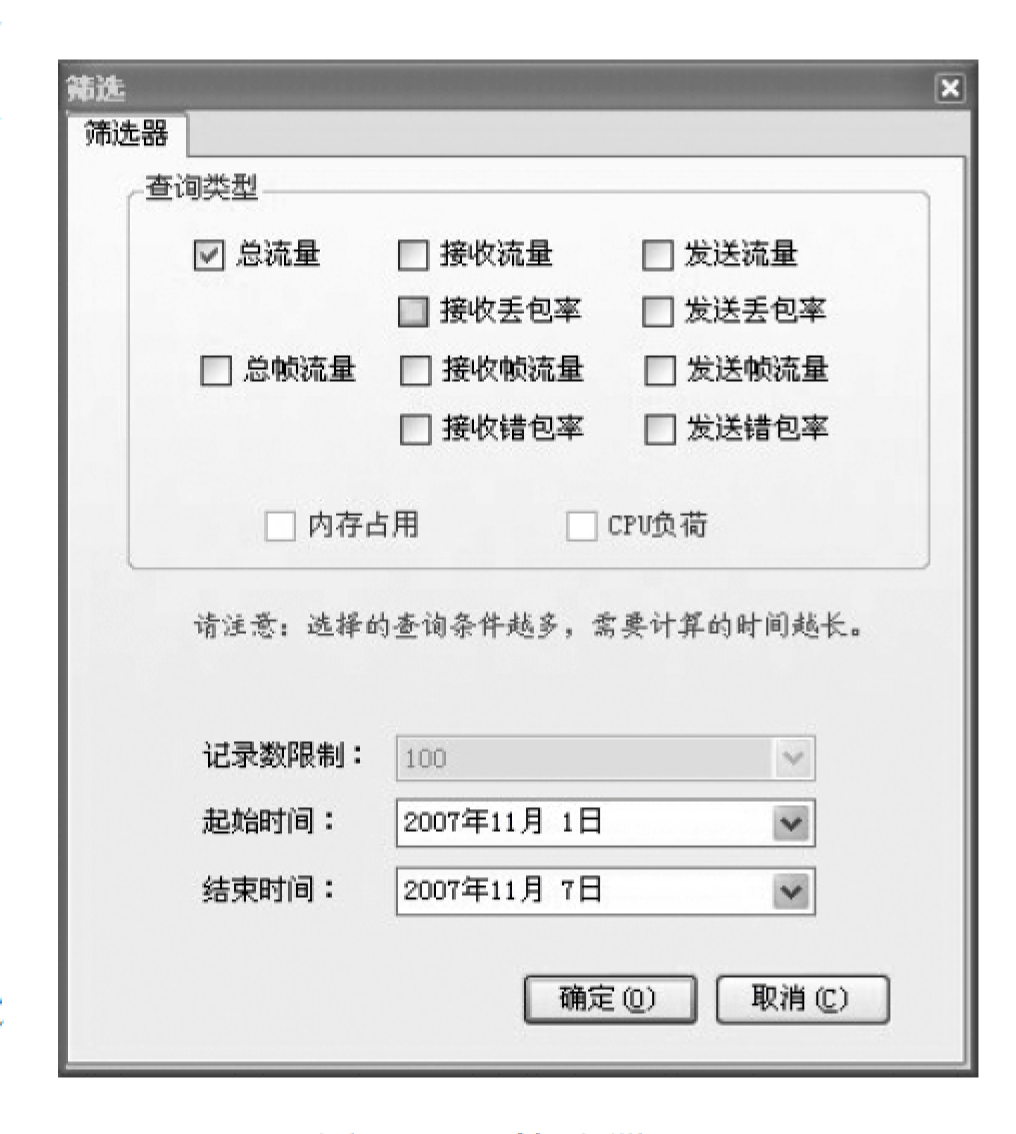


图 5-58　筛选器(2)

5.7.6　设备故障趋势分析

统计当前设备在某时间段内，除 IP-MAC 绑定之外其他 17 个告警项目的告警次数，并以表格、饼图、折线图的方式展示各告警项目



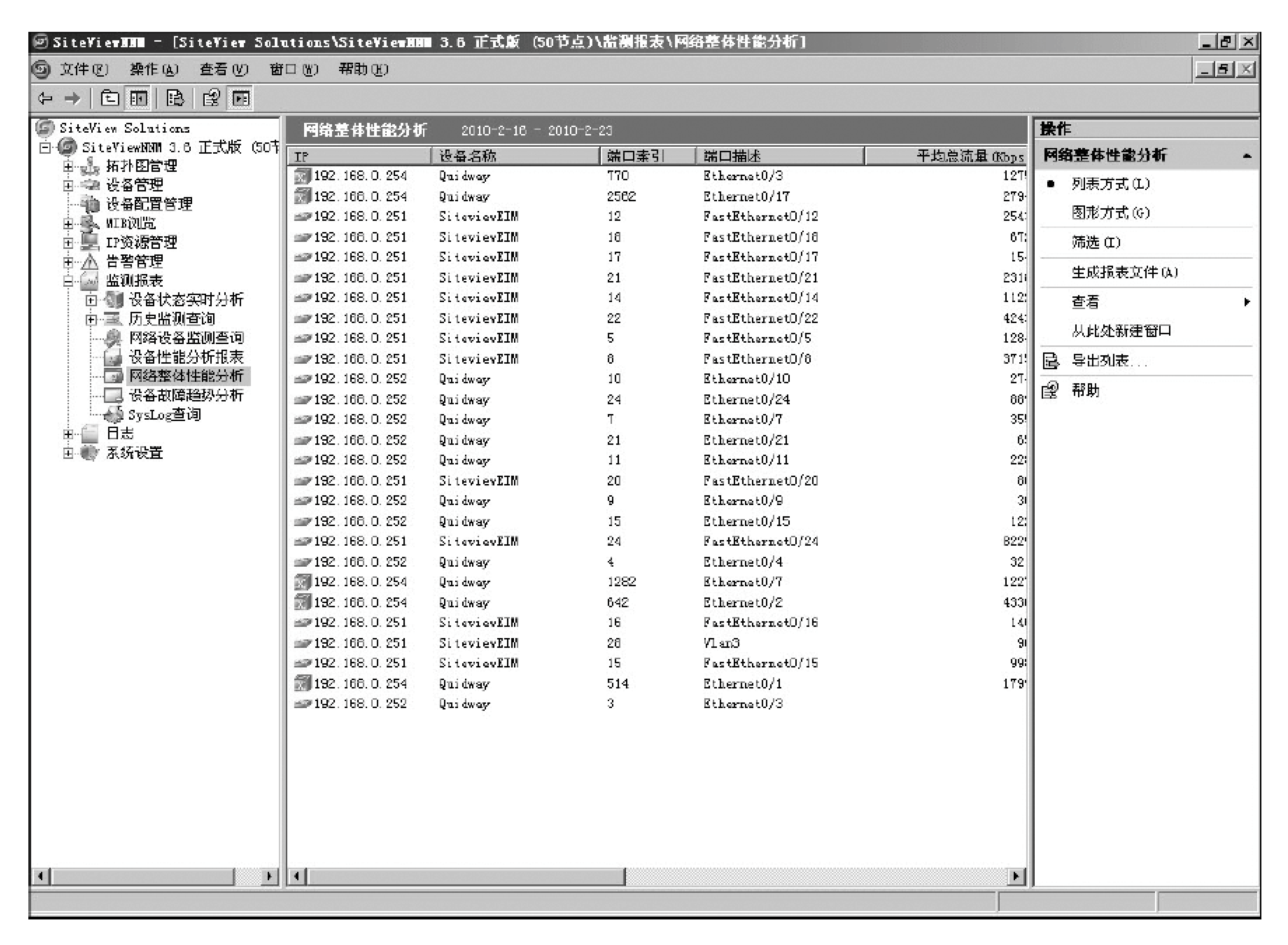


图 5-59　整体性能监测报表

和全部告警次数及其所占的百分比，为用户精确管理网内设备提供重要依据。它与告警管理模块相关，必须要先设置告警，系统产生告警数据后，报表才能做出统计和分析。图 5-60 和图 5-61 分别对设备的故障趋势做了报表和折线图的表示。

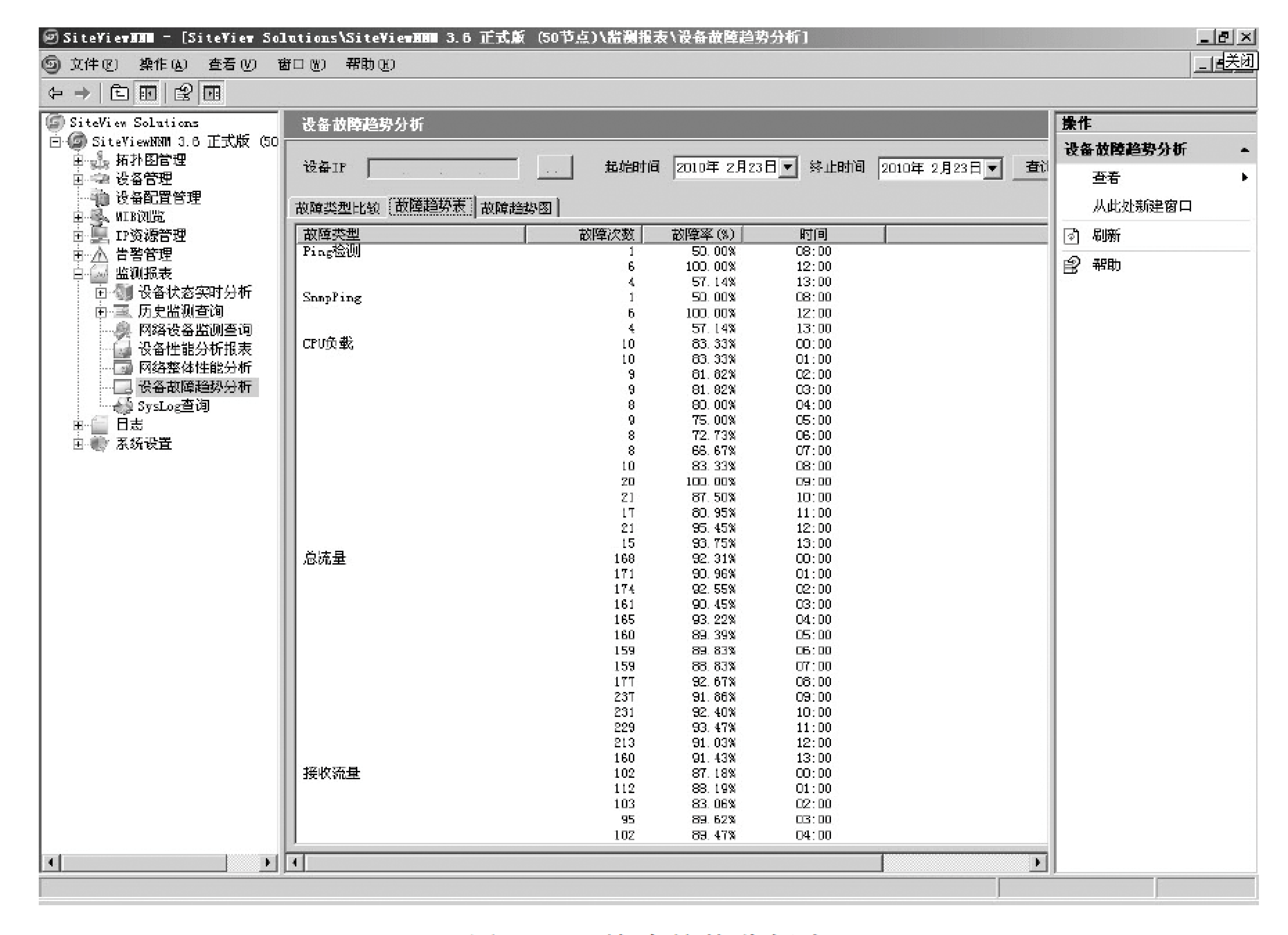


图 5-60　故障趋势分析表

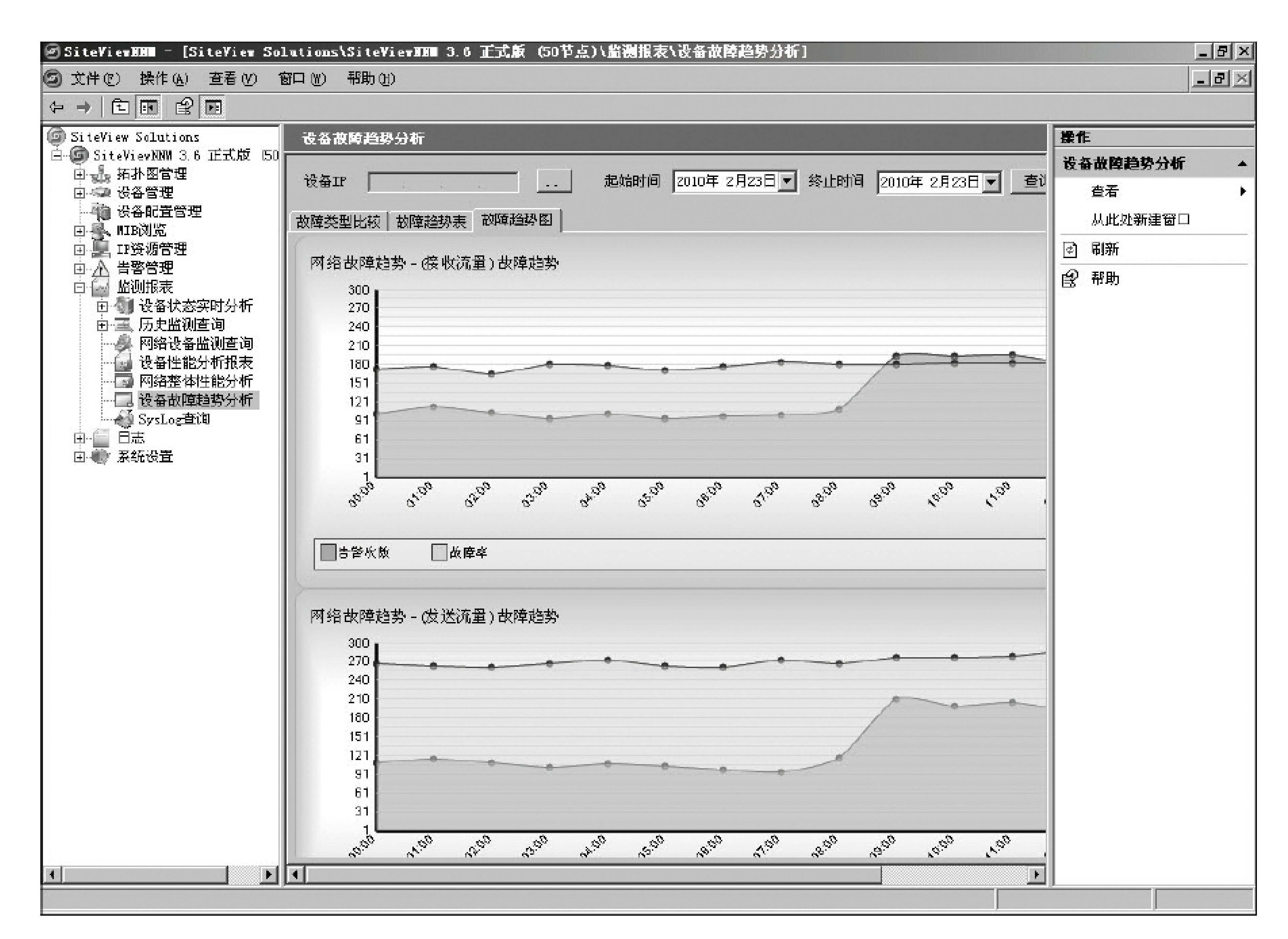


图 5-61　故障趋势分析图

本章小结

本章介绍了基于SNMP协议的网络管理系统概念、构成要素、功能和常见的软件产品。重点介绍了SiteView NNM网络管理系统的功能。要求熟练掌握SiteView NNM的拓扑图管理、设备管理、IP资源管理、警告管理、检测报表管理设置要点与操作过程，通过SiteView NNM反映的数据了解网络的运行情况。同时通过对SiteView NNM网络管理系统的使用，对其他网管软件有一定的理解，以期达到触类旁通的目的。

本章习题

1. 简述基于SNMP协议的网络管理组成要素、布局结构。
2. 简述SiteView NNM网络管理系统常见的管理功能。
3. 简述SiteView NNM控制台的个构成部分的主要作用。
4. 在实验环境中安装SiteView NNM，并用它进行网络管理。
5. 谈一下基于SNMP协议的网络管理软件与你用过的其他网络软件的不同之处。

第6章

局域网监控软件

【本章重点】

掌握"网路岗"管理软件的安装、设置、管理、使用方法与技巧。了解网络监控的基本内容、网络监控软件的体系结构及常见的网络通信的技术特征。

网路岗是目前国内领先的上网监管软件,只需要通过一台计算机即可监控整个网络的网络活动,是政府机构、企事业单位和校园、网吧上网的必备管理软件之一。考虑到成本、网络规模、使用要求,对于一般的网络管理员来说,网路岗软件功能比较丰富、操作比较方便,在一般计算机网络中的应用非常广泛,因此本书选择介绍网路岗软件。

网路岗软件界面友好、操作简单,同时也具有很强的实用性,对复杂的网络结构有很强的解决能力,适合绝大多数代理软件、防火墙、路由器等上网模式的网络。自2002年推出第一代产品以来,通过不断地完善与改进,网路岗软件不断升级,在产品监控功能不断增强的同时,产品的稳定性也得到了大幅度地提高,并被广泛的应用。

6.1 网路岗软件的安装与验证

6.1.1 软件的安装

1. 系统要求

- 操作系统:Windows XP/2000/2003/7。
- CPU:Pentium 4或赛扬2.0GHz以上。
- 硬盘空间:建议硬盘空闲空间不低于10GB。如果监控100台机器的邮件,建议采用30GB以上的硬盘。

通常情况下,监控机器越多,网络流量越大,需要的配置就越高。

2. 安装步骤

- 打开安装光盘,按默认选项操作即可成功安装。
- 安装完成,运行网路岗软件出现的界面如图6-1所示。

3. 软件配置

(1) 绑定网卡(如图6-2所示)。

绑定网卡就是选择从哪块网卡抓信息包。



图 6-1　网路岗界面

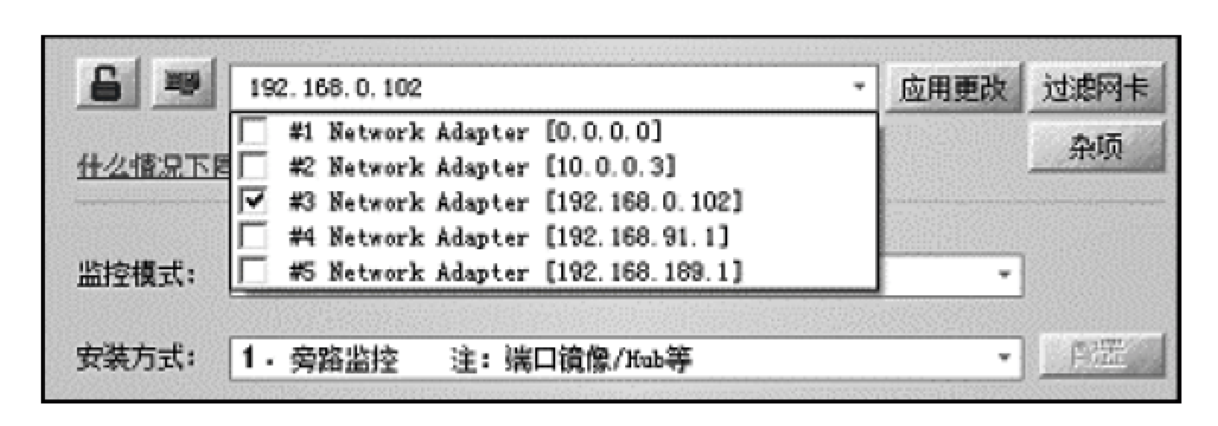


图 6-2　绑定网卡

绑定网卡的注意事项：

- 若安装网路岗的计算机有多块网卡，则选择时要谨慎，选错网卡，网路岗不但监视不了任何信息，同时也不能对目标机器进行任何控制。
- 选择网卡时，应选择内网段的网卡，而不能选择接入 Internet 的网卡。

提示：默认情况下，系统获取通信数据包的网卡和发送封堵包的网卡是同一块，但可以设置信息过滤网卡，以便系统通过另外一块网卡来发送封堵包以控制目标机器。

有一种情况，必须启用信息过滤专用网卡。设置镜像端口来实现对数据包监视后，却不能和局域网其他机器进行通信（假定该机器 IP/网关配置正确），也就是说，所设置的镜像端口只能接收信息包，而不能发送数据包，镜像端口是单向的。针对这类情况，建议再添一块网卡，作为网路岗的信息过滤专用网卡。

在图 6-2 中单击“过滤网卡”，则在如图 6-3 所示的“高级设置”对话框中配置信息过滤专用网卡。配置时，信息过滤网卡、镜像端口和被镜像端口必须在同一交换机的同一 VLAN 中。

（2）查看监控效果。

测试监控效果时，先观察能否实时监控到目标机器上网页面的情况，如图 6-4 所示。

（3）配置内部网段。

进入“网络定义”栏目，设置起始 IP 及结束 IP。这里需要提醒的是：只有当需要监控多个子网时，才需要手动配置内部 IP 范围，如图 6-5 所示。

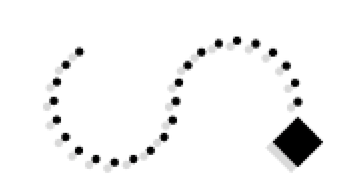




图 6-3　"高级设置"对话框



图 6-4　后台监控服务图标



图 6-5　网络定义中的内部网 IP 设置

如果采用非透明代理服务器软件实现多机共享上网，那么必须在该处输入代理服务器的 IP 地址(内网 IP 范畴)。另外，如果网内有邮件服务器等内网资源，也需要在上面输入其 IP，才能监控到内网机器访问内网资源的情况，如图 6-6 所示。

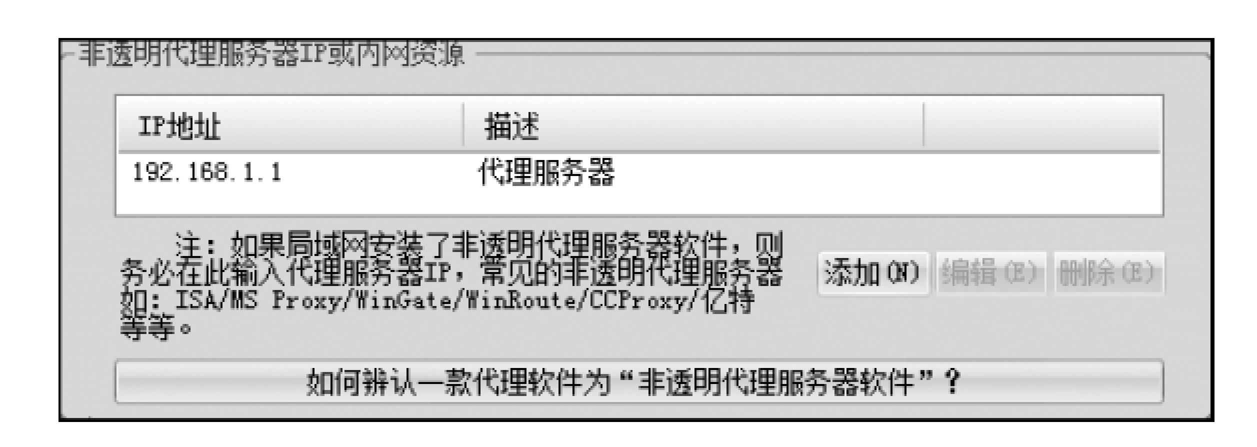


图 6-6　非透明代理服务器设置

定义因特网出口 IP 的设置，一般为被监控机器上网的网关 IP（或代理 IP），属于内部网 IP 范畴，只针对单网段有效果。如果添加 IP 时，能正确输入出口 IP 所对应的 MAC 地址，系统会在很短的时间内自动恢复被封机器的上网通道，如图 6-7 所示。

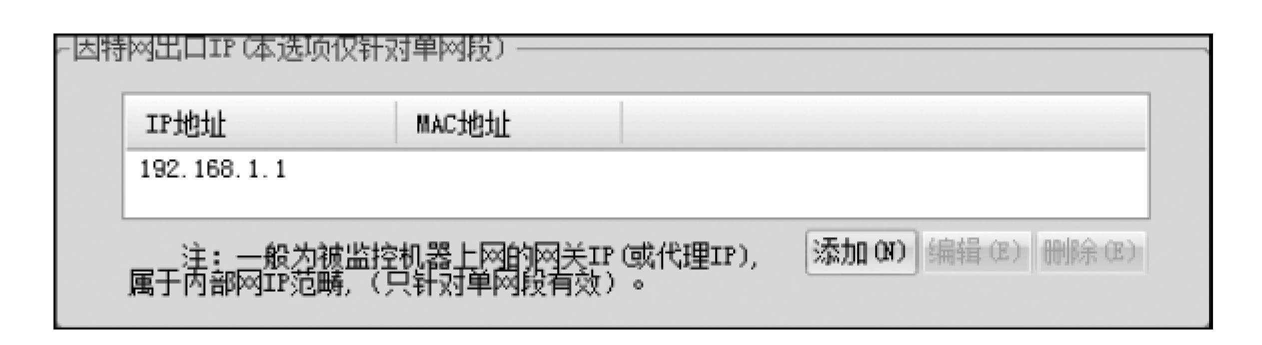


图 6-7　因特网出口 IP 设置

6.1.2　验证安装是否正确

1. 检查目标机器的监控状态

选择“常规”→“首页”命令，监控模式选择“基于网卡 MAC”，先看看是否有机器信息，如果没有，就用“电脑列表”功能查看每台机器，单击某台机器前的小图标，该机器的状态可循环改变，如图 6-8 所示。在“电脑清单”窗口下可单击“搜索局域网内的电脑”，也可以搜索局域网内的电脑。



图 6-8　目标机器的监控状况

其中，✓表示该机器被监控，vip 表示该机器不被监控，✗表示该机器不被监控但也不允许上网。

2. 检查被监控机器的上网情况

选择“文件”→“现场观察”命令，在确保被测试的机器处于✓状态后，让该机器上网，如 www.google.com 等，并留意“现场观察”窗口中是否有对应的网络带宽流量信息；如果该窗口中能正确显示目标机器的上网情况，说明对该机器的监控是正常的，对该机器的封堵也将起作用。此外，如果流量图表上的指针出现摆动，则说明有通信流量，如图 6-9 所示。

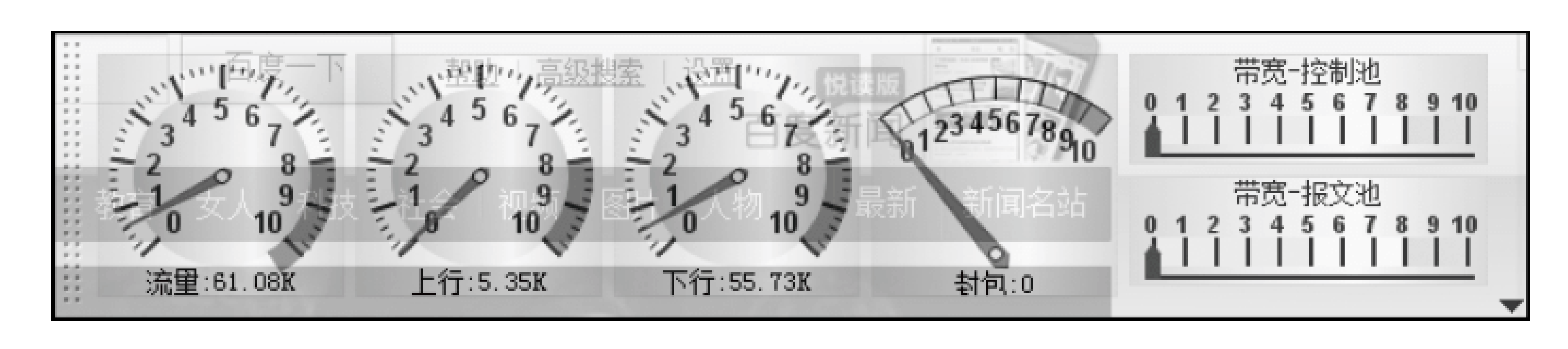
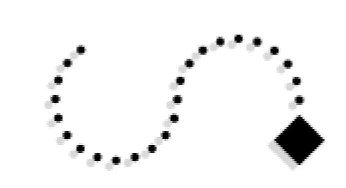


图 6-9　流量图表

3. 封锁目标机器上网

选中被测试的机器，在“现场观察”窗口中单击“上网规则”右侧的“打开”按钮，则打开“编辑‘上网规则’”对话框，在其中选择“端口过滤”，如图 6-10 所示。在 80 端口上打上钩



（注：如果网络采用代理上网，则上网端口可能不是 80，这就需要添加新的端口，并打钩），下部的封锁时间段全为绿色，单击 “更新规则”→ET 按钮，最后单击“保存设置”按钮使设置生效。



图 6-10　封堵端口设置

设置完毕后，再次让被目标机器上网，并检查“现场观察”窗口中的记录显示。

通过上述三个步骤的测试，可以有效地检测出产品安装是否成功。

6.2　网路岗各种监控模式介绍

6.2.1　基于网卡监控

基于网卡监控就是以网卡 MAC 为依据，根据网卡 MAC 地址确定被监控的信息内容的身份。由于每台机器的网卡 MAC 相对固定，被监控的机器不易修改，如果网络规模不大，建议管理员将该网络监控模式列为首选。

在这种网络监控模式下，被监控的机器更换新的网卡后，网路岗会重新检测到新的 MAC，因此，新网卡将被当作新加入的机器来处理，在此提醒管理员注意。

基于网卡网络监控模式的操作步骤如下：

（1）选择网络监控模式为“基于网卡 MAC”，如图 6-11 所示。

（2）设置监控对象，如图 6-12 所示。如果图 6-12 左边部分为空，则需要先启动监控服务，选择绑定正确的网卡，然后，单击“搜索局域网内的电脑”按钮，输入正确的 IP 地址

监控模式：1．基于网卡MAC　注：可实现跨VLAN监控

图 6-11　网络监控模式

范围，开始搜索。即使不用“搜索邻居”功能，如果有机器上网，新发现的机器同样可以自动加入；每一目标机器都有相应的目录，默认情况下，新机器都放入目录 New Folder 中。

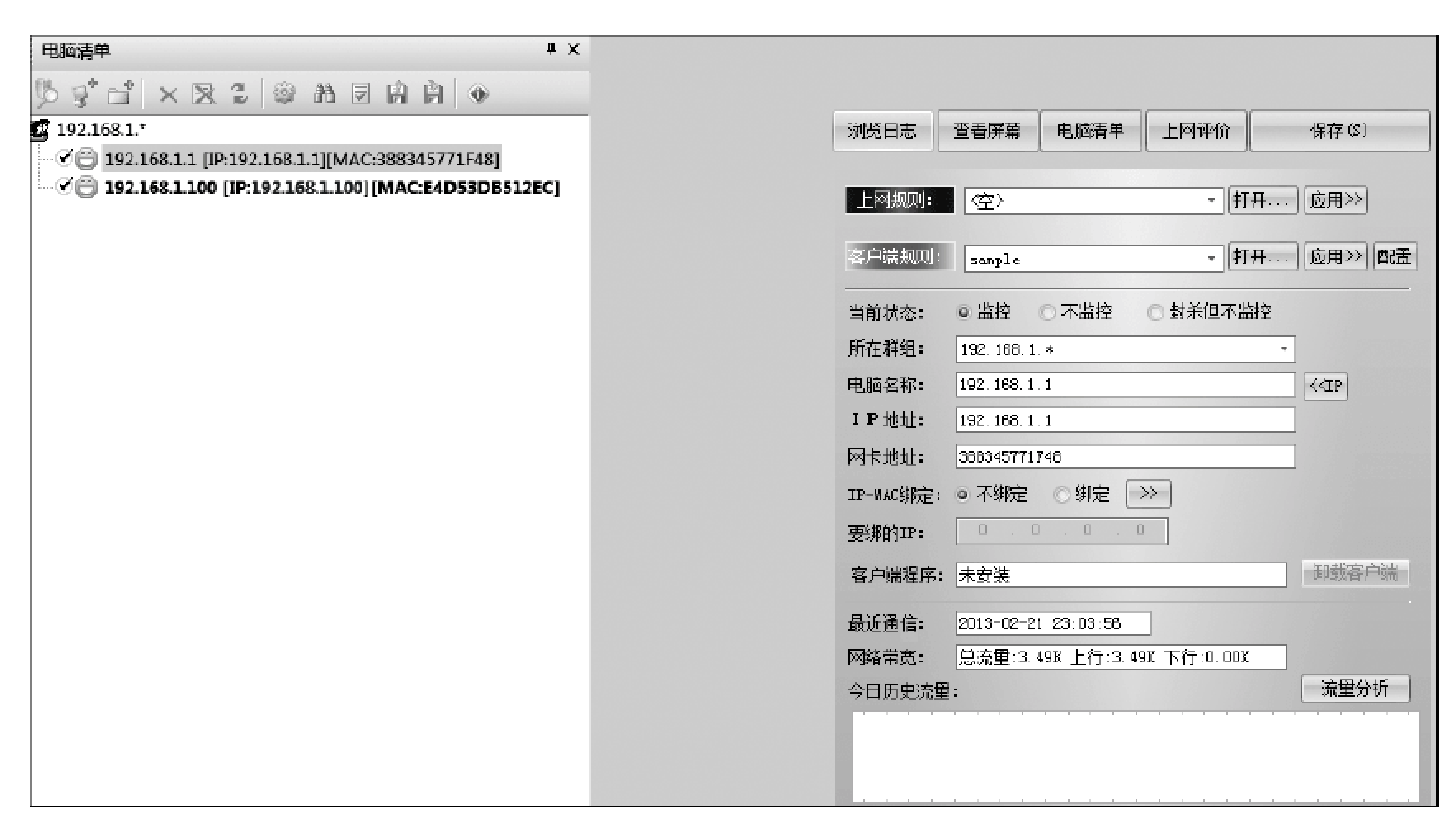


图 6-12　监控对象界面(1)

在“电脑清单”窗口下有一个小的工具栏，下面介绍这些工具的功能。

“搜索局域网内的电脑”：自动探测指定 IP 范围内的机器信息(IP 地址/网卡 MAC)。

“手动添加电脑”：手动添加电脑，可添加到某一群组。

“创建新的群组”：创建新的群组，以便对目标机器进行分组管理。

“删除选中条目”：删除选中的一个或多个目标，也可用来删除空的群组。

“清空电脑列表”：清空电脑清单中的电脑。

“刷新电脑列表”：刷新电脑清单中的电脑。

“电脑自动分类设置”：可把电脑按 IP 地址范围加入群组或者套用同样的上网规则。考虑到电脑列表中会出现非常多的电脑，如果电脑全部搜集到一个“群组”下面，管理起来就会比较困难，所以，第八代提供了专门的“新电脑自动归类”处理功能。

“查找电脑”：如果目标机器太多，就可以用此功能来找出要找的机器。

“解析：IP→电脑名”：当新机器被加入时，机器名默认为其 IP 地址，如想将 IP 地址转变成机器名，就可使用此功能。

“导入：磁盘文件→电脑列表”：将导出的机器及规则配置信息从指定的文件加入当前机器列表中。

“导出：电脑列表→磁盘文件”：将目标机器的信息及其对应的规则配置导出到自定义的文件中。

“电脑列表信息”：列出了电脑前监控状态图标的含义和处于各种监控状态电脑的统计。

6.2.2　基于 IP 监控

基于 IP 监控的定义：以 IP 地址为依据，并以此 IP 来确定所监控的信息的身份。

当网络复杂、电脑数量多的时候，在基于 IP 监控的方式下，管理员可定义一个 IP 范围段来作为一个管理对象。可能只关心某一范围内机器的上网情况，对这些机器做统一的控制，不一定非要具体到某台机器。

基于 IP 网络监控模式的操作步骤如下：

(1) 选择基于 IP 的网络监控模式，如图 6-13 所示。

(2) 设置监控对象，如图 6-14 所示。

监控模式：　3．基于IP　注：适合大型网络

图 6-13　网络监控模式



图 6-14　设置监控对象界面

6.2.3　基于账户的网络监控模式介绍

“基于账户”启用后，被控电脑浏览网页时，会跳转到“上网认证”界面，如图 6-15 所示。上述页面的用户可以自定义，具体方式请联系开发商。

账户模式又分为两种情况。

- 活动目录(域)情况：该模式的前提是，在网络内安装并启用了活动目录(Active Directory)，上网用户需要先通过域登录才可以访问互联网资源；每个上网用户都有自己的账户和密码，一个账户可在多台机器上登录。针对这类情况，网路岗没有必要重新定义一套账户来管理上网，而只需要从活动目录中获取账户信息，通过现有的账户管理上网即可。



图 6-15　“上网认证”界面

- 系统自定义情况(多在网吧、宾馆客房中使用)：在此网络监控模式下，目标机器首次上网时，如访问外部网站，在 IE 窗口中将会出现要求身份验证的对话框，当验证通过后，在屏幕上方自动弹出计时窗口，表明目标机器的在线情况，这时候，目标机器才可以正常上网、收发邮件等。

选择基于账户的网络监控模式，如图 6-16 所示。

设置监控对象，在“电脑清单”窗口单击“手动添加电脑”按钮，弹出“新建账户”对话框，在此设置账户的账号和密码等信息，如图 6-17 所示。

新建账户后的“电脑清单”窗口。此后，该用户上网时将被要求输入账户名和密码，否则不能上网，如图 6-18 所示，在此还可以限制该账户每天的上网时间。

监控模式：　2．基于账户　　注：需开启上网评价功能

图 6-16　监控模式界面

新建账户
账户信息
用户账号：
账号密码：
用户描述：
确定　取消

图 6-17　“新建账户”对话框



图 6-18　监控对象界面(2)

监控方式的选择：

“基于网卡 MAC”是主要推荐的一种监控方式，适合网络规模在 5000 台计算机以下的情况。

“基于 IP”监控主要用于电脑规模大、控制要求不高的网络；基于 IP 监控时，用户可以定义范围 IP，以简化对监控目标的管理。

“基于账户”主要针对一些特殊行业，如酒店、宾馆、网吧等。

6.3　全局定义/规则

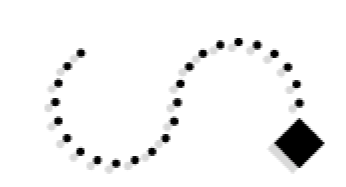
1. 网络定义

(1) 定义内部网段，如图 6-19 所示。

只有出现多网段/多子网的情况，才需要定义内部网段。定义网段时，一般要求定义每个需要监控的 IP 段，但是，也可采用简化的定义方式，如输入 192.168.0.1—192.168.1.255，这样只需要输入一次。

(2) 设置代理 IP 或内网资源，如图 6-20 所示。

如果采用非透明代理服务器软件实现多机共享上网，那么必须在该处单击“添加”，再



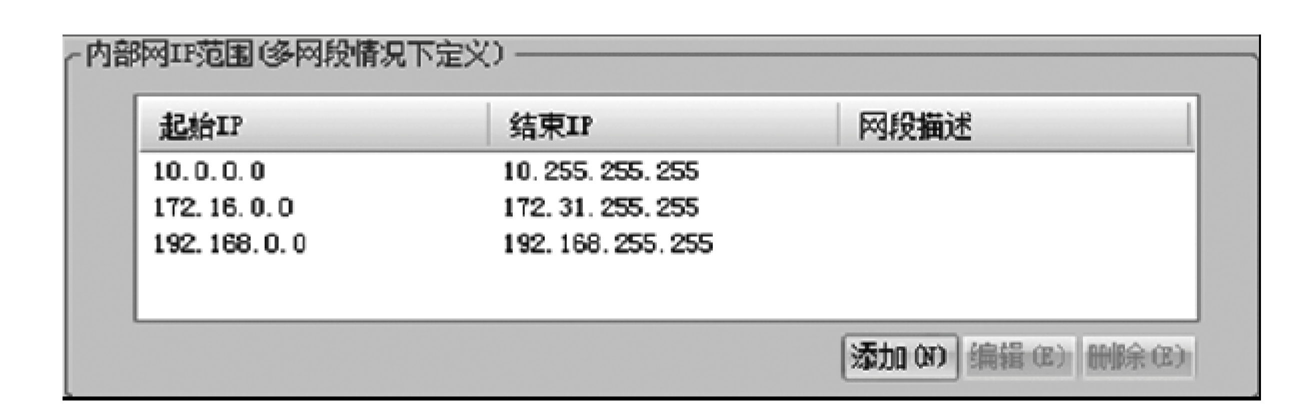


图 6-19　定义内部网段

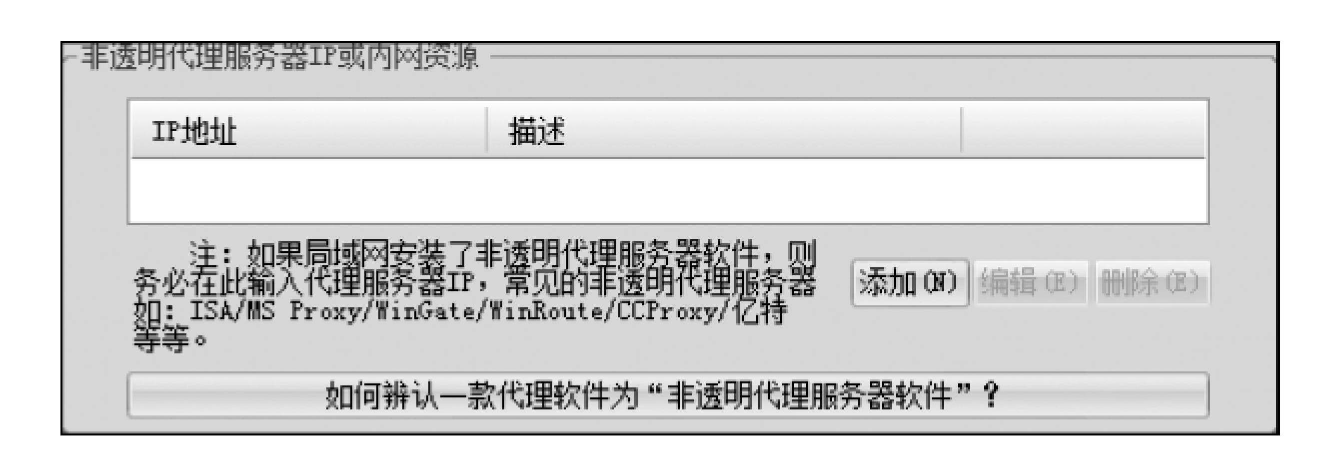


图 6-20　设置代理 IP 或内网资源

输入代理服务器的 IP 地址(内网 IP 范畴)。另外，如果网内有邮件服务器等内网资源，也需要在上面输入其 IP，才能监控到内网机器访问内网资源的情况。

2. 不规范上网行为

可以通过如图 6-21 所示的对话框设置记录哪些不规范的上网行为。



图 6-21　不规范上网行为设置

在图 6-21 中单击“添加”，可以弹出如图 6-22 所示的对话框，补充一些包含敏感信息的网站。

自定义项目

报警类型：访问敏感网站

报警名称：

匹配条件

访问网站的URL包含下面的关键词：

描述：关键词可以是多个，每个关键词之间用小写的逗号隔开。只要符合任何一个关键词就报警。

确定　取消

图 6-22　自定义上网行为

3. 监控端口

监控项目和端口是息息相关的，系统通过对特定端口数据的分析来实现对特定项目的监控，如图 6-23 所示。每一个项目可同时配置三个端口，如用户的网络有一天也许同时有 80、8080、3128 等访问网站的端口的现象出现，这样就需要配置多个端口。

编辑　保存设置　端口自学习(针对非透明代理，如ISA等)

端口名称	端口	缺省值
HTTP		80
SMTP		25
POP3		110
FTP		21
TELNET		23

图 6-23　监控端口

如果采用非透明代理服务器软件实现共享上网，且代理端口并非 80，那么就需要在 HTTP 的端口 80 后面增加一个端口值。此时，可以在如图 6-23 所示的窗口中选择端口名称，单击“编辑”，则弹出如图 6-24 所示的编辑端口界面，多个端口以逗号分隔。

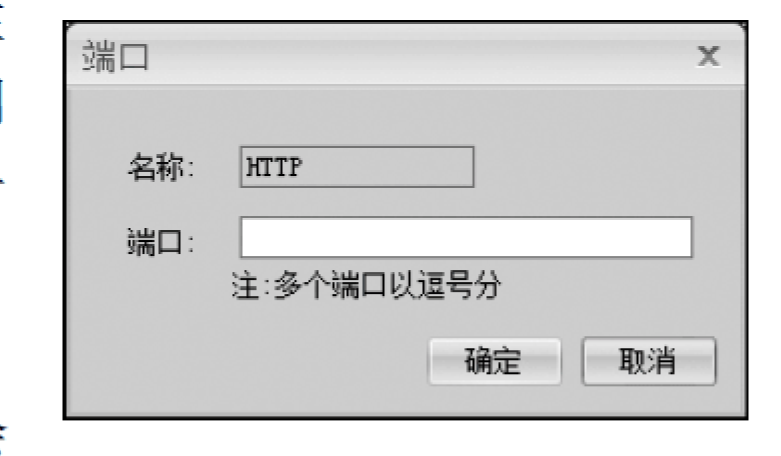


图 6-24　编辑端口

4. IP 黑名单

当系统检测到有机器恶意扫描外网端口时，系统会自动将其归入黑名单，也可手动添加到黑名单，如图 6-25 所示。无限期归入黑名单，也可设置临时有效期，在有效期过后，该机器又恢复正常。

5. IP 白名单

可以添加一些 IP 地址到 IP 白名单，处在白名单内的 IP 地址将无条件放行，处于不监控状态，如图 6-26 所示。

6. 空闲 IP

通常，网络管理员在给网内机器分配完 IP 后发现有些 IP 范围段是空闲的，短期内用



图 6-25　IP 黑名单设置

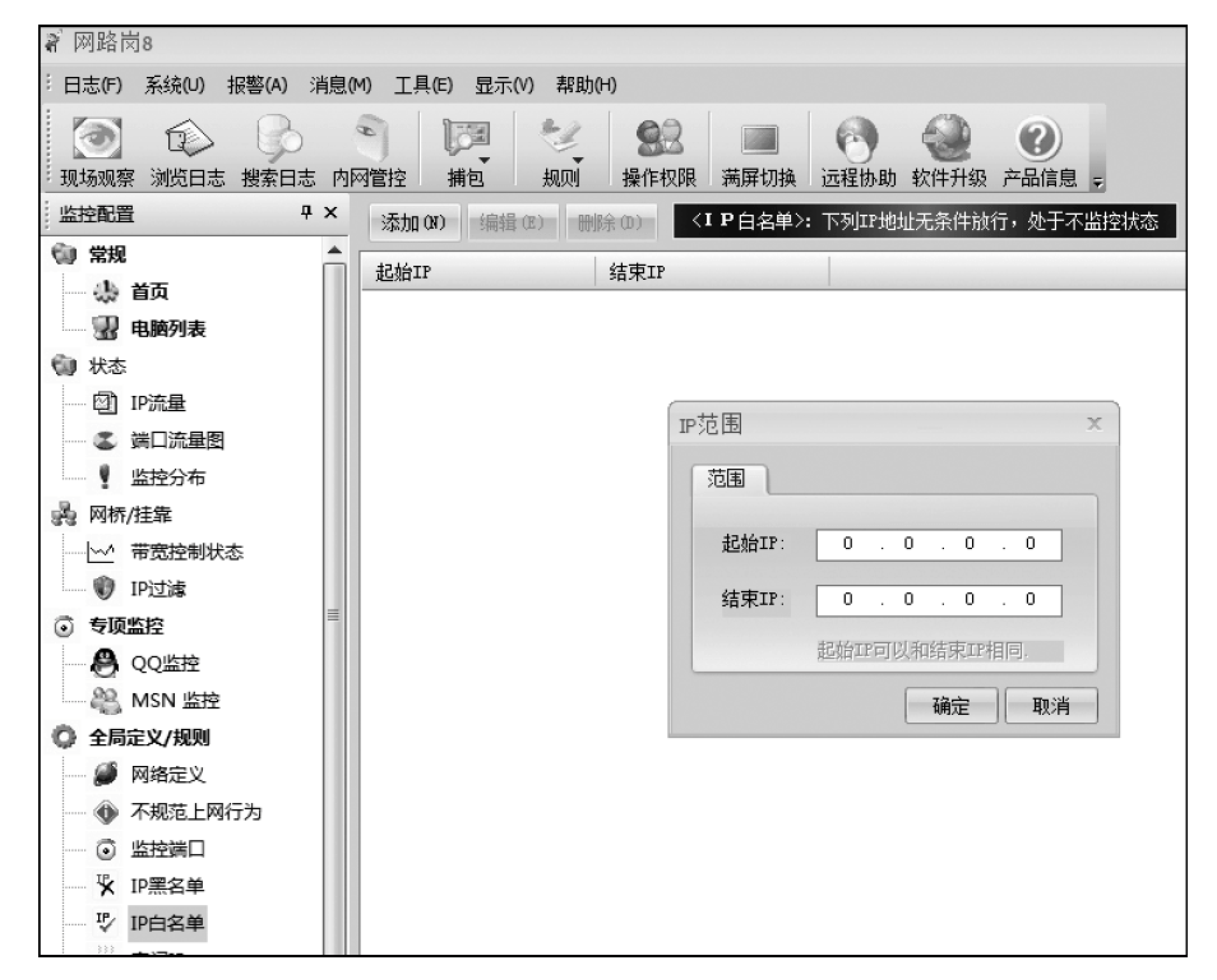


图 6-26　IP 白名单设置

不上;同时网管也不想让这些 IP 被使用,那么,利用空闲 IP 防止计算机 IP 被私下更改就非常有效,如图 6-27 所示。

7. 报警

单击"报警",则弹出如图 6-28 所示的对话框。



图 6-27　空闲 IP 设置

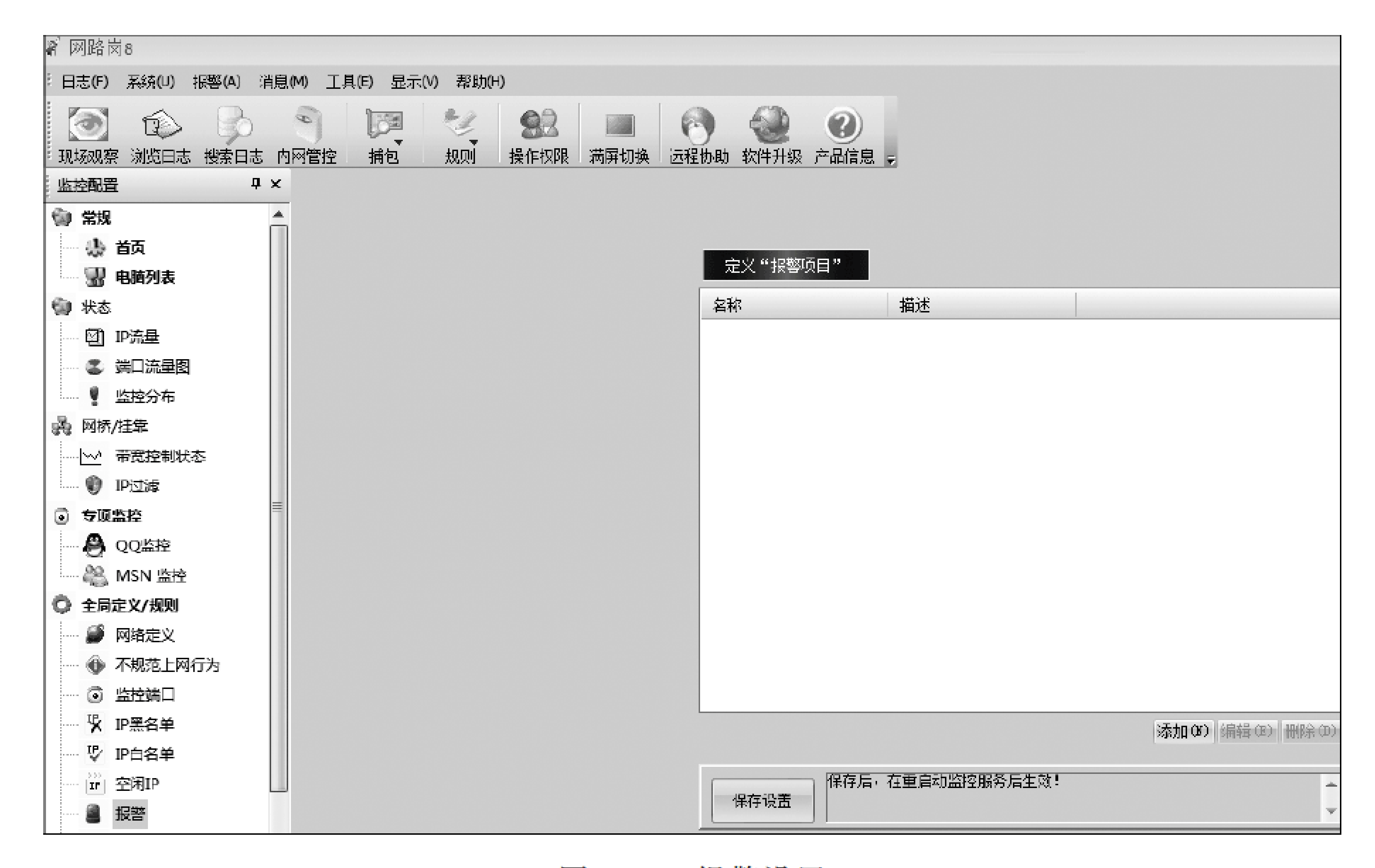


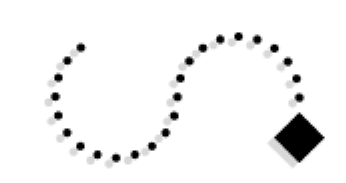
图 6-28　报警设置

选择“添加”，则弹出“报警项目定义”对话框，如图 6-29 所示，可添加需要加入监控的 URL 关键词。定义关键词的时候，建议输入最具代表性的词。此功能可用来封堵某些特定网站。

8. 监控项目

可以在此设置常见网络活动监控项目和外发资料的监控项目，在相应项目前的方框内打钩即可，如图 6-30 所示。

除了上述的项目之外，还可以做监控项目自定义。以过滤 UDP 登录方式的 QQ 为例，这里设置的 Port 8000—8001 是针对每条通信的外网端口的。其他通信端口的过滤



报警项目定义

报警类型：访问敏感网站

报警名称：

匹配条件

访问网站的URL包含下面的关键词：

描述：关键词可以是多个，每个关键词之间用小写的逗号隔开。只要符合任何一个关键词就报警。

报警有效时间：

报警的同时，自动将其加入IP黑名单

临时，有效时间：10 秒　永久

确定　取消

图 6-29　报警项目定义

常见网络活动监控项目

访问网站(HTTP)

发送邮件(SMTP))

接收邮件(POP3)

ICQ(英文聊天)

腾讯QQ(中文聊天)

异地上传或下载文件(FTP)

登录异地电脑(TELNET)

单个IP通信流量

Msn Messenger

Yahoo Messenger

自定义项目...

外发资料的监控项目

通过网站发邮件或粘贴文章

利用OutLook等邮件工具发邮件(包括附件)

利用OutLook等邮件工具接收邮件(包括附件)

使用FTP工具上传文件

图 6-30　监控项目界面

设置方式类似。单击“自定义项目”，则弹出“自定义监控项目”对话框，如图 6-31 所示。

如果能够了解某个病毒/游戏/聊天软件的通信包规律，通过自定义项目，就可以让网路岗来提醒用户哪台机器在做什么敏感的事情。

如果系统检测到符合上述条件的通信包，就会在现场观察窗口中显示出来，并记录到日志文件中。

9. 监控时间

监控时间安排，如图 6-32 所示。用户可根据需要设置过滤启用时间，该时间是针对

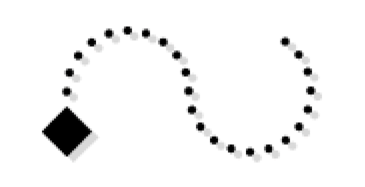
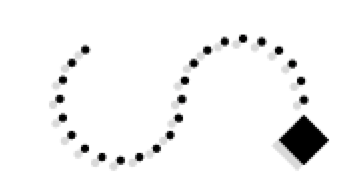


图 6-31　自定义监控项目

所有过滤项目的总体控制的。该处显示的监控时间是全局的，在非监控时间段，监控服务会完全不做任何控制，尽管服务还处于运行状态。



图 6-32　监控时间段设置



6.4　上网规则

1. 网页过滤

选择工具栏里的“规则”选项,在弹出的菜单中选择“编辑上网规则”。在弹出的对话框中选择“网页过滤”标签。网页过滤主要是针对 URL 地址的过滤,对内容不予过滤,如图 6-33 所示。



图 6-33　网页过滤

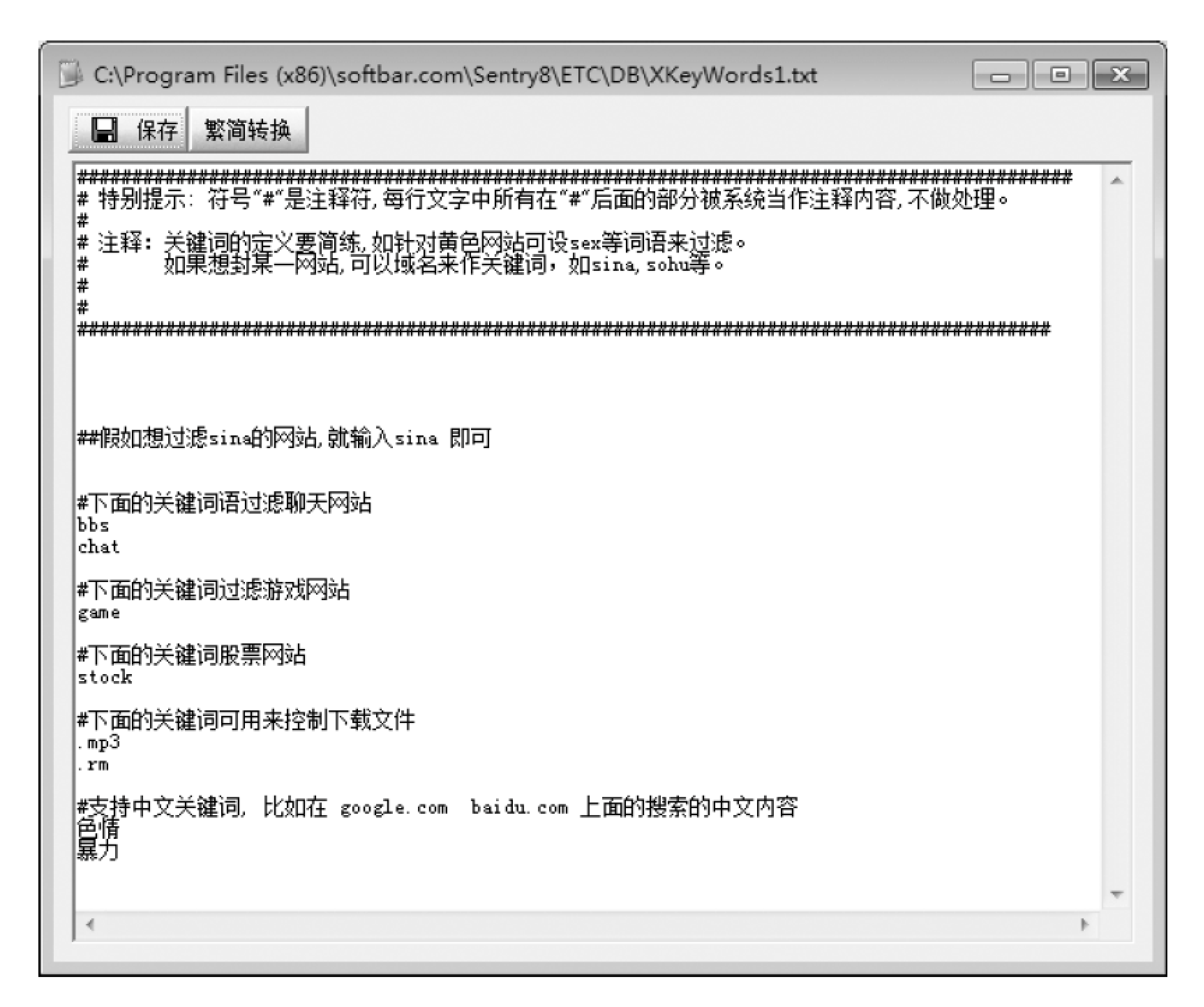
举例说明:

在禁止网站列表中输入“暴力”,以防被控机器在搜索网站上以该关键词来搜索,如图 6-34 所示。

在只允许访问的文件中输入 google.com 和 google.com.hk 只能上 google,如图 6-35 所示。

2. 流量限制

首先说明,只能检测到上网带宽数据而不能实现对带宽的管理和分配。尽管如此,根


C:\Program Files (x86)\softbar.com\Sentry8\ETC\DB\XKeyWords1.txt

保存 繁简转换

```
################################################################################
# 特别提示：符号"#"是注释符，每行文字中所有在"#"后面的部分被系统当作注释内容，不做处理。
#
# 注释：关键词的定义要简练，如针对黄色网站可设sex等词语来过滤。
#       如果想封某一网站，可以域名来作关键词，如sina，sohu等。
#
#
################################################################################



##假如想过滤sina的网站，就输入sina 即可


#下面的关键词语过滤聊天网站
bbs
chat

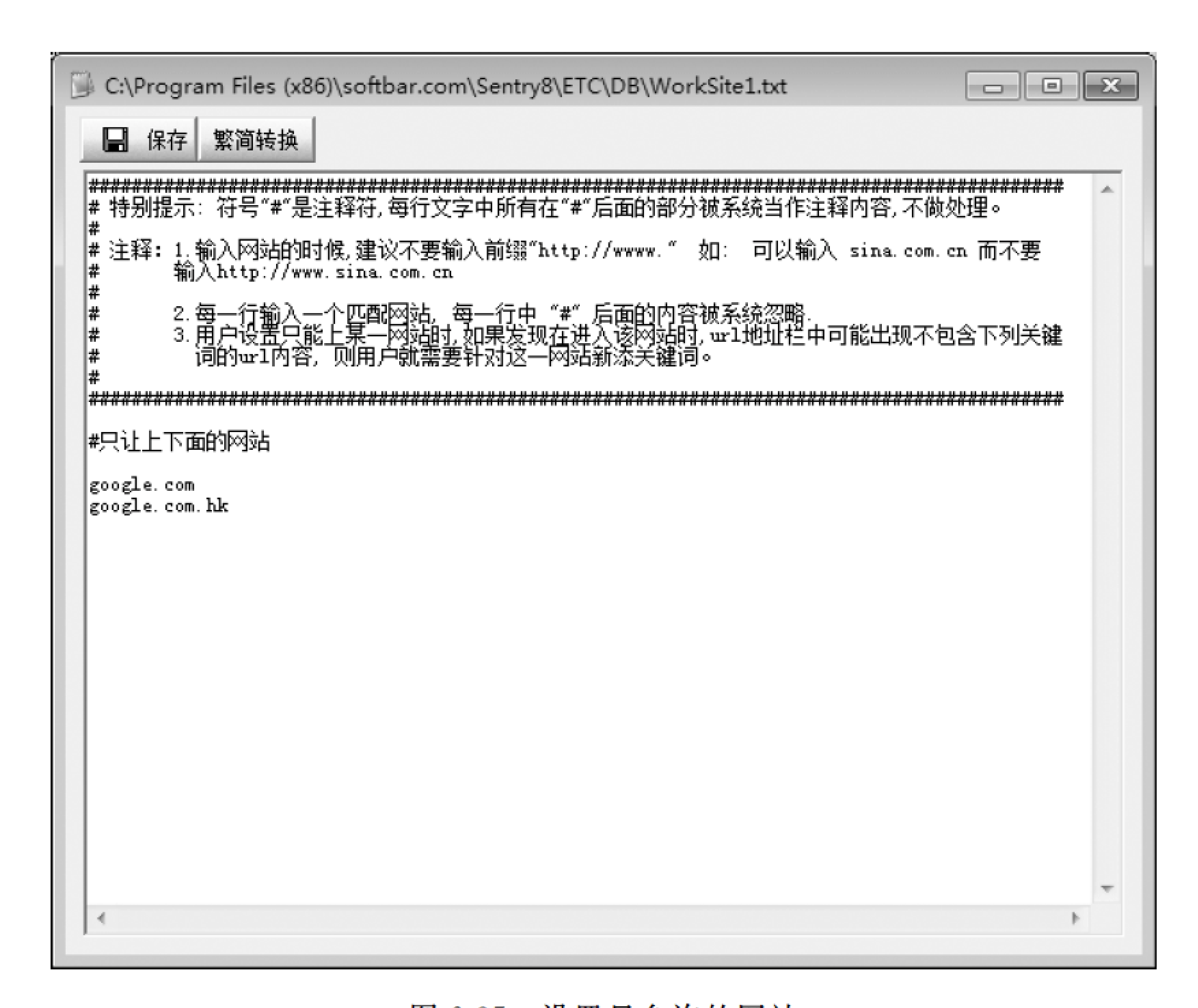
#下面的关键词过滤游戏网站
game

#下面的关键词股票网站
stock

#下面的关键词可用来控制下载文件
.mp3
.rm

#支持中文关键词，比如在 google.com  baidu.com 上面的搜索的中文内容
色情
暴力
```

图 6-34　关键词设置


C:\Program Files (x86)\softbar.com\Sentry8\ETC\DB\WorkSite1.txt

保存 繁简转换

```
################################################################################
# 特别提示：符号"#"是注释符，每行文字中所有在"#"后面的部分被系统当作注释内容，不做处理。
#
# 注释：1.输入网站的时候，建议不要输入前缀"http://www." 如： 可以输入 sina.com.cn 而不要
#       输入http://www.sina.com.cn
#
#       2.每一行输入一个匹配网站，每一行中"#"后面的内容被系统忽略.
#       3.用户设置只能上某一网站时，如果发现在进入该网站时，url地址栏中可能出现不包含下列关键
#         词的url内容，则用户就需要针对这一网站新添关键词。
#
################################################################################

#只让上下面的网站

google.com
google.com.hk
```

图 6-35　设置只允许的网站

据客户的要求，该软件提供了对流量的限制功能，如图 6-36 所示。例如，限制某台机器每天只能有多少兆字节的上网流量，超过这个数字，系统就会自动断网。



图 6-36　流量限制界面

"流量限制"选项卡显示的累计流量是动态的，便于及时观察到客户机的流量。

3. 下载类型

网路岗可以设置禁止下载的文件类型，在相应的类型前打钩即可，如图 6-37 所示。单击"添加"，还可以增加禁止下载的文件类型。

4. 网络软件

可以设置过滤掉一些网络软件，在相应项目前打钩即可，如图 6-38 所示。

5. IP 过滤

IP 过滤是针对 Internet 上各类资源的 IP 地址的过滤，进行设置时，需要对 IP 有全面的了解。事实上，全球 IP 地址的分配是有一定规定的，相关知识可在网上搜索到，搜索关键词请用"IP 地址分配"，利用这些规定，可以设置某些地区的网站不可以上。

某些大型网站，如 Yahoo、Sina 等都有很多的 IP 地址，因此，不能简单通过一两个 IP 地址来封锁该网站。

IP 过滤的设置界面与网络软件的过滤界面类似，设置方法也类似，如图 6-39 和图 6-40 所示。



图 6-37　禁止下载文件类型的设置



图 6-38　网络软件过滤设置



图 6-39　IP 过滤界面

```
C:\Program Files (x86)\softbar.com\Sentry8\ETC\DB\XIP1.txt
保存 繁简转换
##########################################################################################
# 特别提示: 符号"#"是注释符,每行文字中所有在"#"后面的部分被系统当作注释内容,不做处理。
#
# 注释: 可以定义某一范围内的IP,也可定义具体的IP, 下列定义是合法的:
#        202.96.134.100 - 202.96.134.255
#        202.96.134.*
#        202.*.*.*
#        202.96.134.135
##########################################################################################
##############################请单行输入信息##############################################
```

图 6-40　IP 过滤设置

6. 端口过滤

为方便控制,网路岗专门收集了端口列表,可供选择。在如图 6-41 所示的过滤选项卡中,单击"添加"按钮进行添加,也可选中某项端口然后删除。

封堵端口是略专业化的功能名词,从本产品一代开始就保留了此功能,是现有客户用得比较多的功能之一。

任何一款网络软件,如果建立在 TCP/IP 通信之上,都会用到端口,如股票软件、FTP 软件、收发邮件软件等,都具备自己的开放端口。因此,通过端口来封锁上网行为是非常有效的。



图 6-41 封堵端口界面

尽管很多软件的端口是软件开发者自定义的，但用户不必担心其改变自身的开放端口，因为，“开放端口”一旦改变，该软件的客户端也必须随之更改，从市场角度看是不现实的。

如果了解 IP 包的话，可利用本系统提供的 IP 分析工具来分析端口。

7. 外发尺寸

对外发尺寸的控制是一种模糊控制，并不能精确到字节数，而且只有在购买的版本具备邮件内容的监控功能时才起作用。如果没有内容监控功能的话，系统无法及时知道外发文件的大小，也就不能在中途进行堵截，具体设置界面见图 6-42。

8. 邮件过滤

邮件过滤并非严格过滤，这是因为如果邮件内容太少，甚至没有，那么系统检测到有邮件发送迹象时，就已经太迟了，该邮件可能已经发送出去了，再去堵截就没有意义了。

尽管如此，针对稍大的邮件的过滤还是有效的，尤其是带附件的邮件，见图 6-43。除此之外，还可以设置只能通过企业邮局收发邮件，或只能发邮件到指定的工作类邮箱。

9. 监控选项

在功能项目选项卡中可根据需要设置目标的监控内容。可以设置监控常见的网络活动、监控外发资料内容或聊天内容等，如图 6-44 所示。

10. 开放端口

可设置只开放指定的端口，如图 6-45 所示。

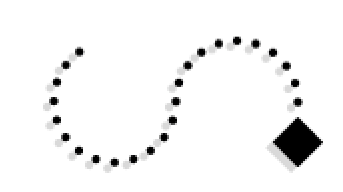




图 6-42　外发尺寸界面

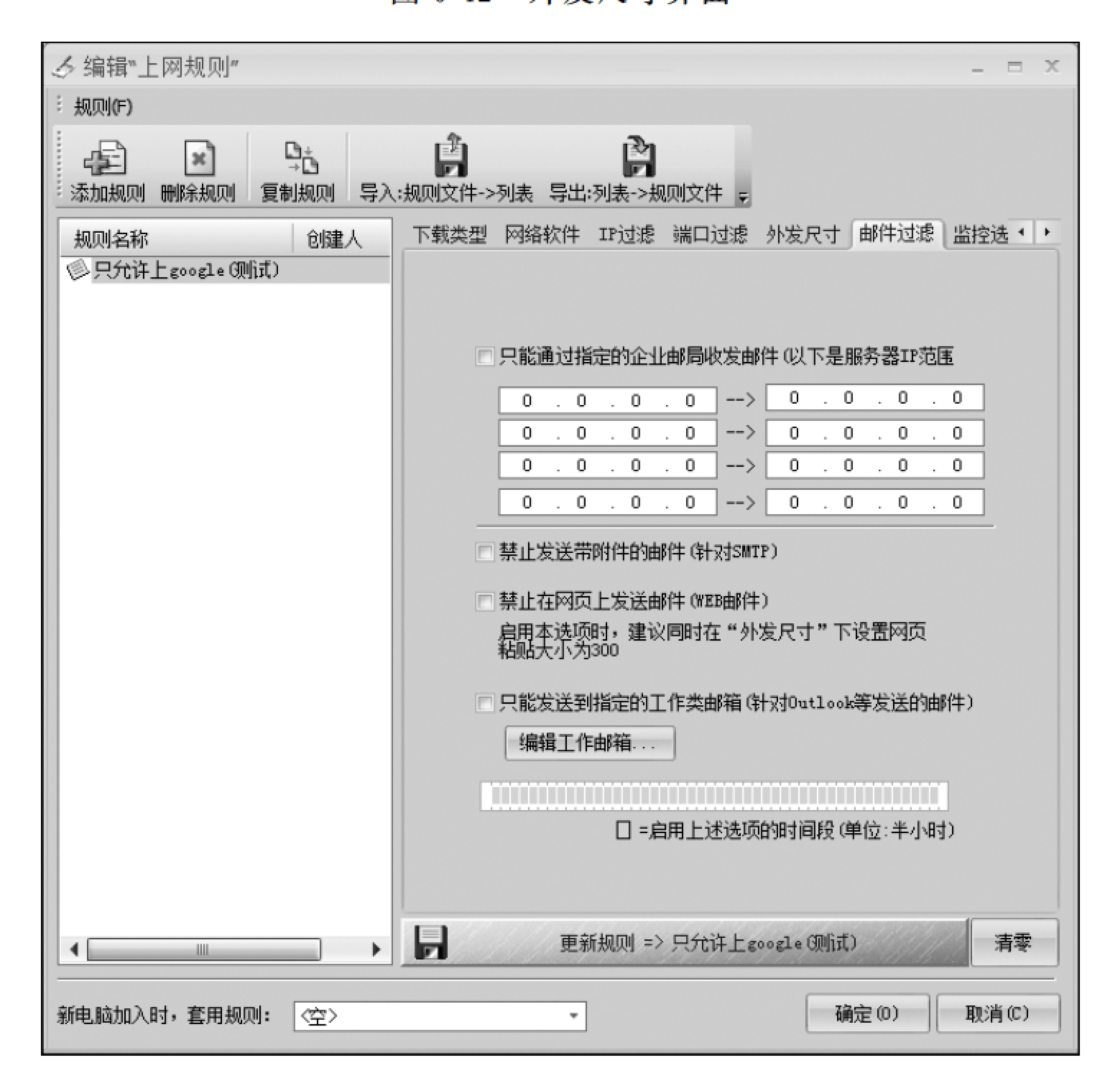


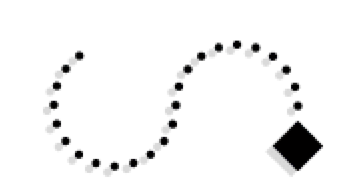
图 6-43　邮件过滤界面



图 6-44　监控选项界面



图 6-45　开放端口设置



11. 启用时段

只有在蓝色时间段，上网规则才起作用，如图 6-46 所示。在蓝色时间段是不是就一定可以上网还难说，主要看其他的选项卡中是否设置了封堵，在如此多的上网规则中，只要有一处封堵，就能起到封堵的作用。



图 6-46　启用时段设置

6.5　客户端规则

6.5.1　客户端规则的安装

选择工具栏里的"规则"选项，在弹出的菜单中选择"编辑客户端规则"。在弹出的"编辑'客户端规则'"窗口中选择"强制安装"，如图 6-47 所示。勾选"强制安装"、"启用'截屏客户端'"(网路岗可以对被监控电脑截屏)和"启用上网评价客户端"(客户端可以接收到上网评价信息)。则客户端电脑上网时会弹出如图 6-48 所示的界面，提示下载安装网路岗客户端软件。

安装成功后，在网路岗管理软件中选中该电脑后，在现场观察窗口中将出现如图 6-49 所示的安装信息。如果不再需要客户端程序，则可以直接单击"卸载客户端"按钮进行卸载。

安装成功后客户端电脑上将出现如图 6-50 所示的"网路岗-上网评价"漂浮窗，在任务栏中出现上网评价图标。



图 6-47　客户端安装设置



图 6-48　客户端上网提示

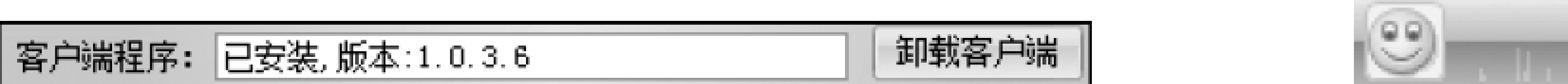
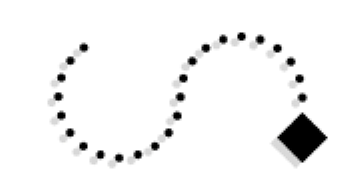




图 6-49　客户端程序已安装信息

图 6-50　"网路岗-上网评价"漂浮窗



6.5.2　客户端规则的设置

1. 截屏配置

可配置针对客户端的截屏时间、截图质量、截图数量等，如图 6-51 所示。



图 6-51　截屏配置

2. 智能截屏

可开启智能截屏，如设置计算机长时间无人操作时不截图，插入 U 盘或光盘后截屏，开启敏感应用程序后截屏等，如图 6-52 所示。

3. 进程控制

可设置客户端禁止运行的程序，如图 6-53 所示。

4. 设备控制

可设置客户端禁用的设备，如摄像头、声卡、光盘等，如图 6-54 所示。

5. 实时评价

可设置进行实时评价的激活条件，如图 6-55 所示。

6. 当天统计

如果客户端行为不当，如当天访问网页过多、QQ 聊天记录数过多等，可以记入日志，如图 6-56 所示。



图 6-52　智能截屏设置



图 6-53　进程控制

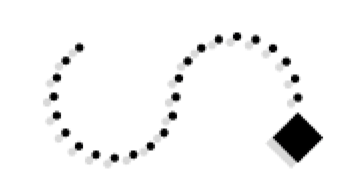




图 6-54　设备控制



图 6-55　实时评价



图 6-56　当天统计

6.6　日志查阅、日志报表及远程控制中心

6.6.1　日志查阅和日志报表

1. 查阅网络活动日志

选择"日志"，单击"浏览日志"，或者直接单击"浏览日志"按钮，可以打开"日志浏览器"窗口。选择目标机器，并选择关心的网络活动，如图 6-57 所示。在查询日志的时候，可以针对所有机器，也可以随意选择目标机器，以显示对应的日志记录。

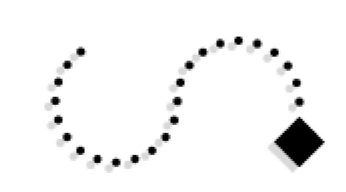
2. 查阅外发文件日志

选择目标机器，在"日志浏览器"窗口的左下侧选择"外发文件"下的项目即可，可查看邮件正文的附件，QQ 传送文件，FTP 传送文件，网页发帖等记录，如图 6-58 所示。

"日志浏览器"中还可以查询聊天内容，统计报表，同时可以做日志的搜索，如图 6-58 所示。

3. 日志报表

日志报表的导出很容易，单击工具栏中的导出结果图标即可导出日志记录到.xls 文件。在此需要注意的是文件名要有针对性，方便日后查询，如图 6-59 所示。



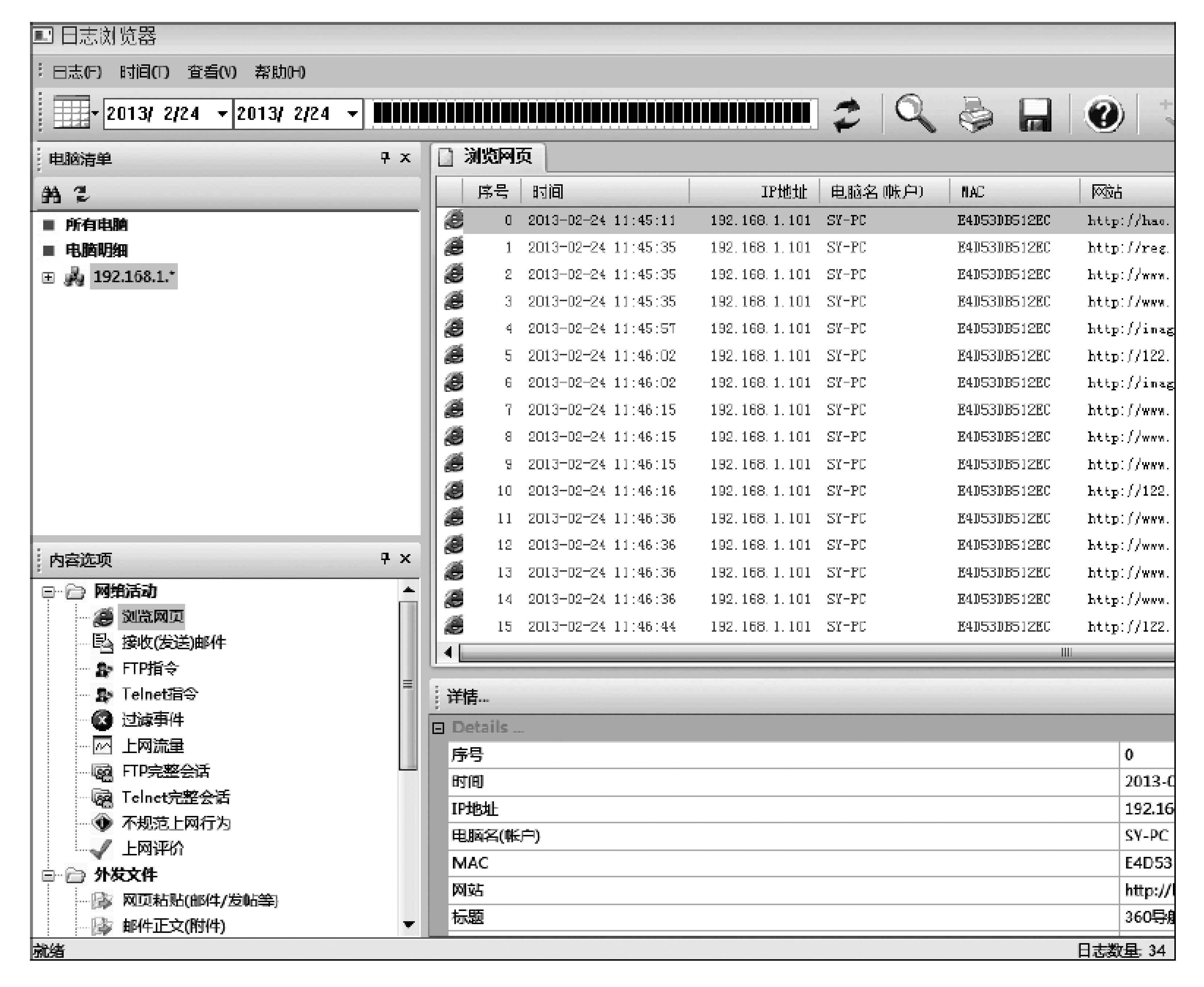


图 6-57　“日志浏览器”窗口



图 6-58　日志浏览器查询项目

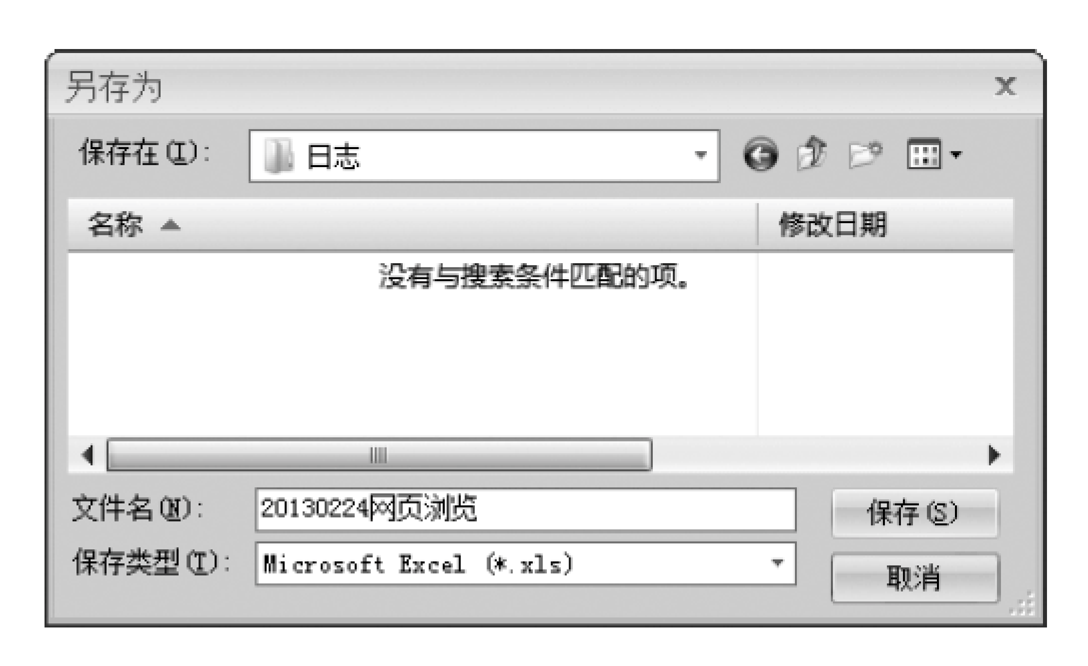


图 6-59　日志报表的导出

6.6.2　远程控制中心

1. 授权

在使用远程日志查阅功能的时候，必须先在监控端进行授权。在网路岗软件的主界面(图 6-61)选择“授权/档案”项目下的“远程＜查阅日志＞授权”，单击“添加”，然后出现如图 6-60 所示界面。

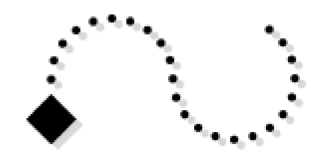


图 6-60　添加用户

授权内容包括用户名、密码、配置程序、查阅日志的权限等,如图 6-61 所示。

2. 安装远程控制中心端程序

安装程序位于光盘中,运行主程序,如图 6-62 所示。



图 6-61　授权界面

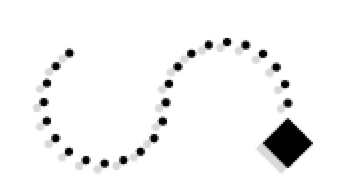


图 6-62　登录界面

首先新建服务器,新建内容包括服务器地址和存放该服务器日志的目录。通过远程控制中心可以选择登录不同位置的服务器。

数据交换口在监控机端有定义,默认是 9010 端口,如果希望更改的话,请在网路岗软件的“授权/档案”项目下单击“远程＜查阅日志＞授权”并做修改后,再重新启动数据交换服务。

在输入用户名和密码后,登录时,可能碰到下面的问题:



（1）错误提示一：“登录服务器失败”。

解决方法如下：

首先，检查服务器 IP 地址是否正确，如果没有问题，再用 Ping 命令检查。如果不能 Ping，则检查监控机上是否安装了个人防火墙软件，如有，则可能需要卸载再试。

如果能够 Ping 监控机，则需要检查数据交换“通信”服务是否已经启动，而且两边的端口是否一致。

（2）错误提示二：“验证名和密码失败”。

解决方法如下：

检查监控机上授权的用户名和密码，如果检查不出任何问题，建议另外新建一个用户名试验。

3. 下载日志

一旦登录成功，就可以通过菜单中的“下载日志”功能来选择下载日志内容，如图 6-63 所示。

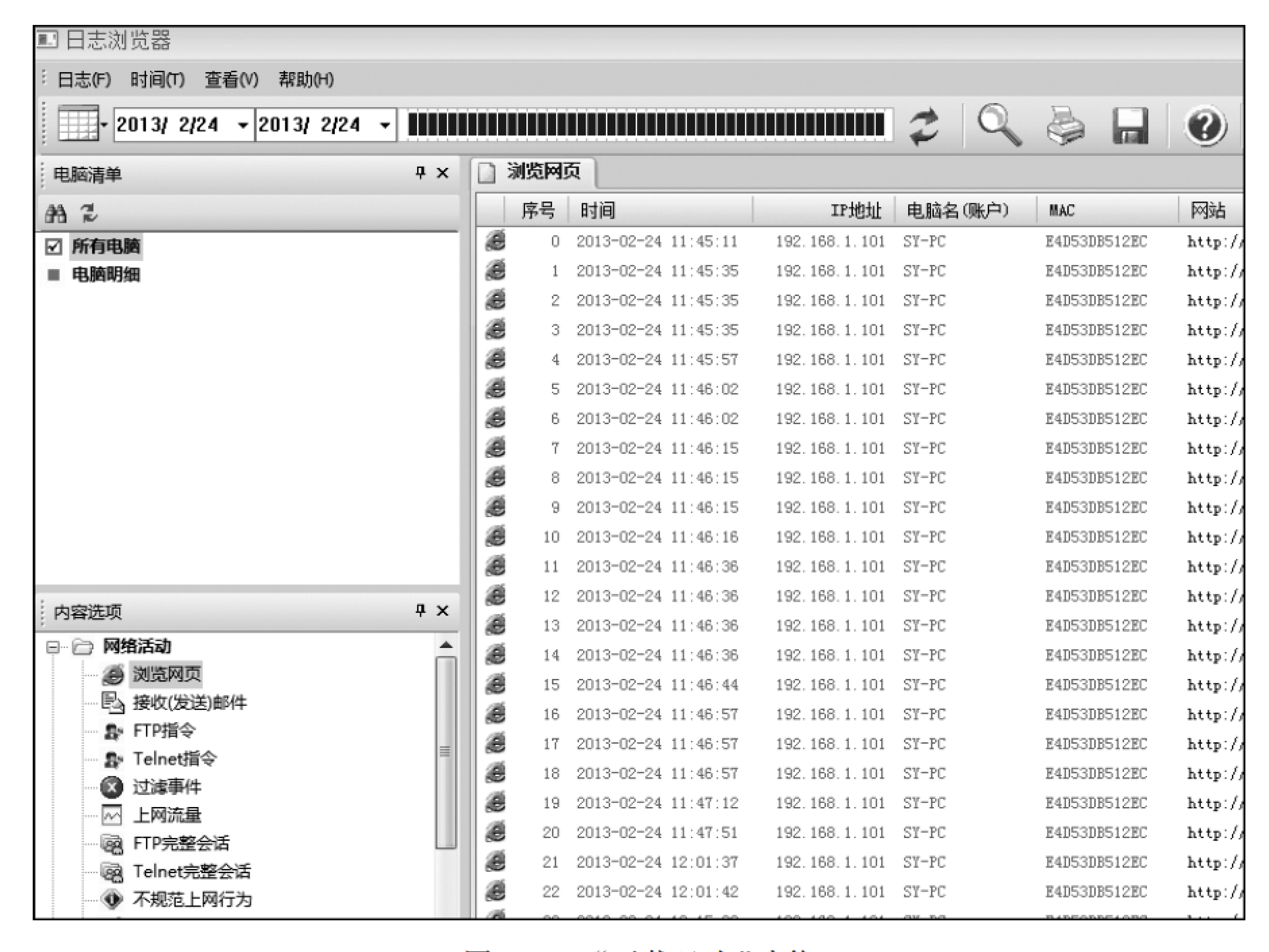


图 6-63　“下载日志”功能

本章小结

本章以网路岗为工具，讲解了网络管理软件的初步使用方法，介绍了此款软件的安装、配置和使用过程。通过学习，要求掌握用网路岗软件对简单网络进行管理的方法和使用技巧，并能触类旁通，使用其他简单网络管理软件对网络进行管理。

本章习题

参照本章所讲，在征得网络管理员同意的前提下，使用网路岗软件对所使用的网络进行管理。

（1）安装网路岗软件。

（2）绑定网卡。

（3）监控模式设置为“基于网卡”模式。

（4）启动所有的后台监控服务。

（5）检验是否安装正确。

（6）封堵某台机器的收发邮件功能，并检验封堵的效果。

（7）查阅网络活动日志和外发资料日志。

（8）进一步熟悉上网规则和客户端规则。

第7章

信息安全

【本章重点】

了解信息安全和加密技术的基本概念和简单的密码技术;了解 DES 和 RSA 密码体制;理解数字签名的基本原理;了解加密技术在电子商务中的应用。重点掌握加密算法的种类、密钥分配与管理方法及数字签名的实现过程。

随着网络技术的飞速发展,网络已经深入到政府、军事、文教、商业等诸多领域,网络在给人们带来方便、快捷的同时,也带来了威胁。计算机犯罪、黑客、有害程序和后门问题等严重威胁着网络的安全。随着人们对计算机网络安全的要求越来越高,这些问题已经引起了普遍关注,成为当今网络技术的一个重要研究课题。

7.1　网络安全概论

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、信息论等多种学科的综合性学科。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不受偶然的或者恶意的原因而遭到破坏、更改、泄露,确保系统能连续、可靠运行,网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义上来说,凡是涉及网络上信息的保密性、完整性、可用性和可控性的理论都属于网络安全的研究领域。

(1) 保密性:信息不泄露给非授权用户。

(2) 完整性:数据未经授权不能进行改变的特性,即信息在存储或传输过程中保持不被修改,不被破坏和不被丢失的特性。

(3) 可用性:可被授权实体访问并按需求使用的特性,即当需要时能否使用的信息。例如,网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

(4) 可控性:对信息的传播及内容具有控制能力。

1. 网络安全内涵

网络安全包括物理安全、系统安全、信息安全、文化安全,网络安全层次图如

图 7-1 所示。

（1）物理安全

物理安全是指保护计算机系统的物理设备、网络连接设备、存储介质及其他媒体。对计算机网络与计算机系统的物理设备的威胁，主要表现为自然灾害（包括地震、水灾、火灾、电磁辐射）以及人为操作失误或盗窃等犯罪行为导致的破坏。

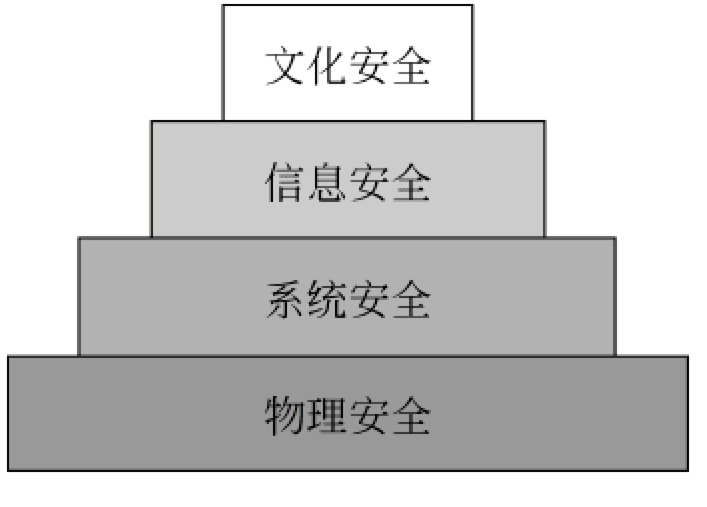


图 7-1　网络安全层次图

危险行为：通信干扰、危害信息的侵入、信号辐射、信号替换、恶劣的操作环境。

防范措施：抗干扰系统、防辐射系统、隐身系统、加固系统、数据备份。

（2）系统安全

系统安全是指保护网络系统、操作系统及数据库系统的安全。系统安全存在的威胁主要表现为对计算机网络与计算机系统可用性与可控性进行攻击，导致网络及计算机不能正常运行。

危险行为：网络被阻塞、资源被非法使用、计算机病毒入侵等使得依赖于信息系统的管理或控制体系陷于瘫痪。

防范措施：安装杀毒软件、防止入侵、检测入侵、攻击反应、系统恢复。

（3）信息安全

信息安全是指对计算机存储介质上存放的数据及在网络中传输的数据安全的保护，对所处理的信息机密性与完整性的威胁，主要表现在加密方面。

危险行为：窃取信息、篡改信息、冒充信息、信息抵赖。

防范措施：加密、完整性技术、认证、数字签名。

（4）文化安全

文化安全是指防止有害信息的传播对我国的政治制度及传统文化的威胁，主要表现在舆论宣传方面，防止和控制非法、有害的信息进行传播，避免公用通信网络上大量自由传输的信息失控。

危险行为：淫秽暴力信息泛滥、敌对的意识形态信息涌入、英语文化的“泛洪现象”对民族文化的冲击，互联网被利用作为串联工具，传播迅速，影响范围广。

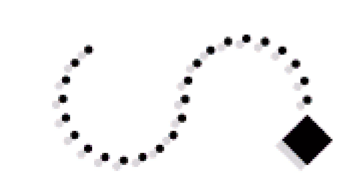
防范措施：设置网关，监测、控管。

2. 网络系统安全领域存在的威胁

（1）操作系统太脆弱，容易受攻击。使用网络离不开操作系统，操作系统是手工编写的，可能存在许多漏洞，有很多网络攻击方式都是针对操作系统的漏洞，入侵计算机来窃取有用信息或阻碍网络信息传输的。

（2）系统被攻击时很难及时发现和制止。网络上的攻击方式一般都是比较隐蔽的，攻击者入侵计算机后造成的影响可能不会马上表现出来。例如攻击者可能会把病毒放入被攻击的计算机中，在很短的时间里大量复制、感染文件，等待病毒发作。当被攻击者发现系统变慢，文件丢失，甚至系统不能正常启动时，为时已晚。

（3）有组织有计划的入侵无论在数量上还是在质量上都呈现快速增长的趋势。早期的计算机入侵主要是编程高手为了显示自己的水平或者证明程序的弊端，基本上都是个



人行为。而现在的入侵比较多的是出于商业或政治上的原因，有组织有计划的入侵可以集中攻击力量，加速入侵的速度，以在更短时间内造成更大的损失或者获得更多的信息。

（4）在规模和复杂程度上不断扩展网络而很少考虑其安全状况的变化情况。网络现在已经渗透到各行各业，很多行业对网络的使用只考虑方便性、开放性，并没有考虑总体安全构想，或对网络安全没有足够重视。应该按网络的规模和网络中数据的重要性来设置网络的安全模式和等级。

3. 网络安全中的主要技术

网络在现代工作生活中扮演了重要的角色，改变了人们的工作方式，加快了人们的工作效率。正是因为它的重要性，所以针对网络的攻击手段随着网络技术的发展也在不断地发展。在网络中采用哪些技术机制才能维护网络的安全呢？

（1）加密技术

加密是提供信息保密最核心、最有效的方法。通常按照密钥类型的不同，加密算法可分为对称密钥算法和非对称密钥算法两种。加密算法除了实现信息的保密性之外，还可以和其他技术结合，例如 Hash 函数，实现信息完整性的检验。

加密技术不仅应用于数据通信和存储，也应用于程序的运行，通过对程序的运行实行加密保护，可以防止软件被非法复制，防止软件的安全机制被破坏。例如，应用程序利用一些加壳软件加上一个外壳，让软件不能被轻易盗版或复制。

（2）访问控制技术

访问控制机制用于控制进入系统的用户对系统资源的使用范围和访问形式，可以防止未经授权的用户非法使用系统资源，这种访问控制机制不仅可以提供给单个用户，也可以提供给用户组的所有用户。访问控制是通过检查访问者的有关信息来限制或禁止访问者使用资源的技术，分为低层访问控制和高层访问控制。低层访问控制是指通过对通信协议中的某些特征信息的识别和判断，来禁止或允许用户访问的措施。

例如，在路由器上设置过滤规则对数据包过滤就属于低层访问控制。高层访问控制包括身份认证和权限确认，是通过对用户口令、用户权限、资源属性的检查和对比来实现的。

（3）数据完整性鉴别技术

数据完整性是指数据是可靠准确的，用来泛指与损坏和丢失相对的数据状态。鉴别是指对信息进行处理的人的身份和相关数据内容进行验证，达到信息正确、有效和一致的要求。一般包括口令、密钥、身份、数据等项的鉴别，系统通过对比验证输入的数据是否符合预先设定的参数，从而实现对数据的安全保护。

这种鉴别技术主要应用于数据库管理系统中，因为企业经营的重要数据都需要保存在一个可靠的系统中，所以保护好企业数据库的安全是非常重要的工作。数据库系统可以根据不同用户设置不同的访问权限，并对其身份及权限的完整性进行严格识别。

（4）身份验证技术

身份验证是系统验证用户是否是合法身份的过程。身份验证包括两种：数字签名机制和 Kerberos 系统。

数字签名机制：数字签名机制一般采用不对称加密技术（后面会详细介绍）。数字签名可以解决 4 种安全问题。

- 否认：事后发送者不承认文件是他发送的。
- 伪造：有人自己伪造了一份文件，却声称是某人发送的。
- 冒充：冒充别人的身份在网上发送文件。
- 篡改：接收者私自篡改文件的内容。

数字签名机制具有可证实性、不可否认性、不可伪造性和不可重用性。数字签名普遍用于银行、电子商务等的身份验证。

Kerberos系统：Kerberos系统是美国麻省理工学院为分布式计算机环境提供的一种对用户双方进行身份验证的方法。Kerberos系统的安全机制在于首先对发出请求的用户进行身份验证，确认其是否是合法的用户，如果是合法的用户，再审核该用户是否有权对他所请求的服务或主机进行访问，其身份是建立在对称加密的基础上的。

(5) 网络防病毒技术

在网络开放的环境下，计算机病毒发展越来越快，并且病毒种类越来越多，也越来越高级复杂，对计算机和网络构成了巨大的威胁。例如，著名的CIH病毒一时间让全世界近六千万台计算机崩溃，由它直接或间接造成的损失达数亿美元，给社会造成了灾难性的后果，因此要重视计算机病毒的防治。网络防病毒技术主要包括预防病毒、检测病毒和清除病毒，具体实现的方法包括对网络服务器中的文件进行频繁地扫描和监测，在工作站上采用防病毒芯片和对网络目录及文件设置访问权限等。

(6) 防火墙技术

防火墙是用一个或一组网络设备，包括硬件和软件，在两个或多个网络间保护一个网络不被另一个网络攻击的安全技术。防火墙通常位于内部网或Web站点与Internet之间的一个路由器或一台计算机上。防火墙如同一个防盗门，保证门内的系统安全。在Internet上，通过防火墙来隔离风险区域与安全区域的连接，但不妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信数据，仅让安全、核准的信息进入，抵制对企业构成威胁的数据进入。

防火墙的主要技术包括数据包过滤和应用代理服务。

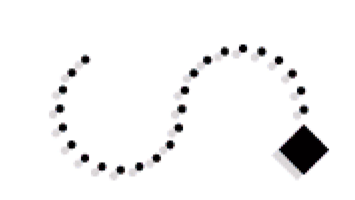
虽然防火墙技术能在内部网络和外部网络之间建立一道安全屏障，但也存在一定的局限性：不能完全防范外部刻意的人为攻击，不能防范内部用户攻击，不能防止病毒或受病毒感染的文件的传输。

(7) 入侵检测技术

入侵检测(IDS)通过对计算机网络或计算机系统中若干关键点收集信息，并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测是防火墙的补充。作为网络安全的核心技术之一，入侵检测技术可以缓解访问隐患，弥补防火墙的不足，将网络安全的各个环节有机地结合起来，实现对用户网络安全的保护。

7.2 加密技术

为什么要对数据加密呢？对哪些数据加密呢？怎样对这些数据加密？这些都是在网络传输数据时需要知道的问题。存放在计算机系统中的数据，每时每刻都受到来自各个



方面的威胁。这些威胁轻则会破坏数据的完整性，重则导致数据完全不可用。数据一旦遭到破坏，对数据拥有者带来的损失将是无法估量的。有没有一种方法能够较好地保护数据，使其即使遭到攻击也能将损失限制在最小范围内呢？

数据加密和数据备份就是实现这个目标的两种最常用也是最重要的手段。前者通过使原本清晰的数据变得晦涩难懂，从而实现对数据的保护。而后者则在数据遭到破坏后，将数据恢复到最近的一个备份点来尽可能减少数据遭到破坏的程度。在数据备份的过程中，数据压缩是一项非常有用的技术，它能够在不影响数据可用性和正确性的前提下大大减少数据所占用的磁盘空间。

几乎任何网络电缆都可能被窃听或监听，攻击者可利用一些网络监听程序或设备截取敏感数据包或其他敏感数据包的复制。假设所有经过网络传输的信息在传输前均被自动地加密，则攻击者将不能完成窃听，网络分析程序收集到的数据包是已加密的数据。如果没有解密密钥，攻击者就不能解释该数据，也就不能知道数据里所包含的真实信息。例如，利用加密板或调制解调器之类的硬件，或是利用位于该传输的两个合法末端的软件执行加密或解密。

大多数用户工作的 PC 都与网络相连，机器里包含了某些攻击者很想得到的存储宝藏（如某公司的销售计划、财务报表或相关商业机密等）的硬磁盘。通过网络对该 PC 的访问几乎是不可阻止的。解决办法是将所有存储于硬磁盘及办公室中的软磁盘上的敏感文件加密。

加密技术是网络信息安全主动的、开放型的防范手段，对于敏感的、重要的数据应采用加密处理，并且在数据传输时也应采用加密传输。本节将着重介绍信息加密技术的一般方法。

7.2.1　数据加密的基本概念

数据加密，就是把原本能够读懂、理解和识别的信息（这些信息可以是语音、文字、图像和符号等）通过一定的方法处理，使之成为一些晦涩难懂的、不能很轻易明白其真正含义的或者偏离信息原意的信息，从而达到保障信息安全的过程。

下面是与数据加密概念相关的几个重要的术语。

(1) 明文(Plaintext,P)：信息的原始形式，也就是加密前的原始信息。明文可以是文本、数字化语音流或数字化视频信息等。

(2) 密文(Ciphertext,C)：通过数据加密的手段，将明文变换成的晦涩难懂的信息称为密文。

(3) 加密过程(Encryption,E)：将明文转变成密文的过程。用于加密的这种数据变换称为加密算法。

(4) 解密过程(Decryption,D)：加密的逆过程，即将密文转变成明文的过程。

(5) 加密过程和解密过程需要遵循的一个重要原则是：明文与密文的相互变换是可逆变换，并且只存在唯一的、无误差的可逆变换。加密和解密是两个相反的数学变换过程，都是用一定的算法实现的。

(6) 密码体制：加密和解密过程都是通过特定的算法来实现的，这一算法称为密码

体制。

(7) 密钥(Key):由使用密码体制的用户随机选取的、唯一能控制明文与密文之间变换的关键参数。密钥通常是一随机字符串。

数据加密和解密的过程如图 7-2 所示。

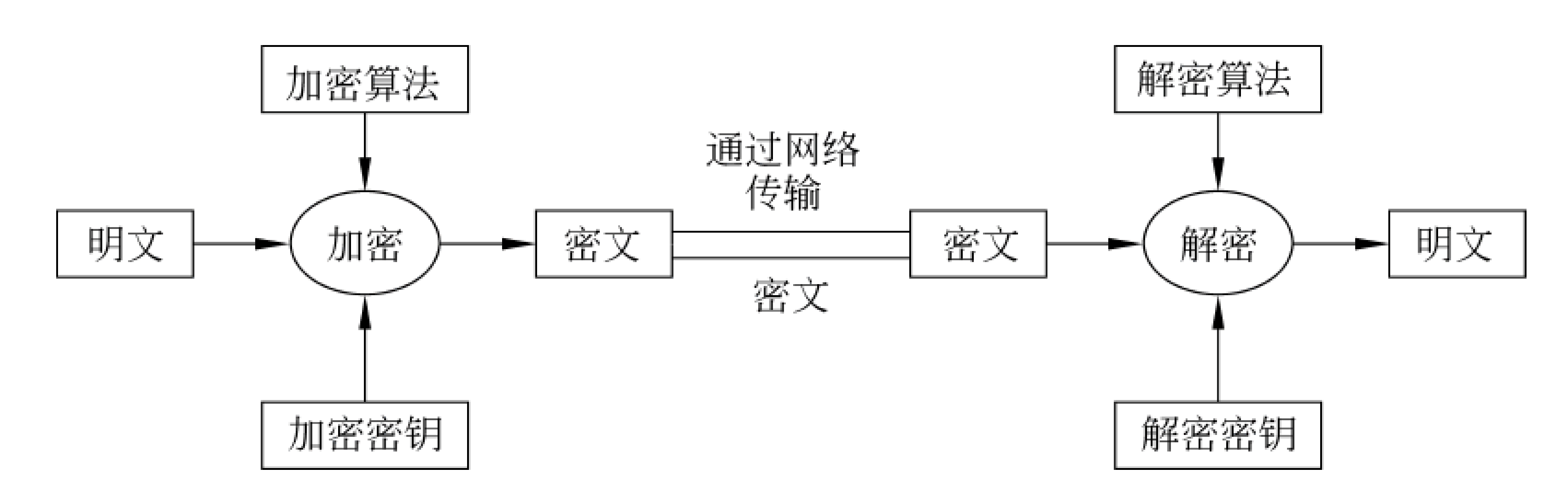


图 7-2 数据加密、解密过程示意图

7.2.2 对称数据加密技术

随着数据加密技术的发展,根据数据加密的方式,可以将密码技术分为对称数据加密技术和非对称数据加密技术。

对称加密,又称为密钥加密,是指加密和解密过程均采用同一把秘密钥匙,通信时双方都必须具备这把钥匙,并保证这把钥匙不被泄露。一旦密钥泄露,只要获得密钥的人就可以利用这把钥匙加密或解密,原来加密过的密文就不具有任何保密性了。所以对称密钥加密技术的关键就是要保存好密钥。

通信双方采用对称加密技术进行通信前,必须先商定一个密钥,这种商定密钥的过程称为分发密钥。发送方使用这一密钥,并采用合适的加密算法将所要发送的明文转变为密文,然后在网络中传送给接收方,密文到达接收方后,接收方用解密算法(通常是发送方使用的加密算法的逆运算),利用双方约定的密钥将密文转变为与发送方一致的明文。

采用对称加密技术进行通信的过程如图 7-3 所示。

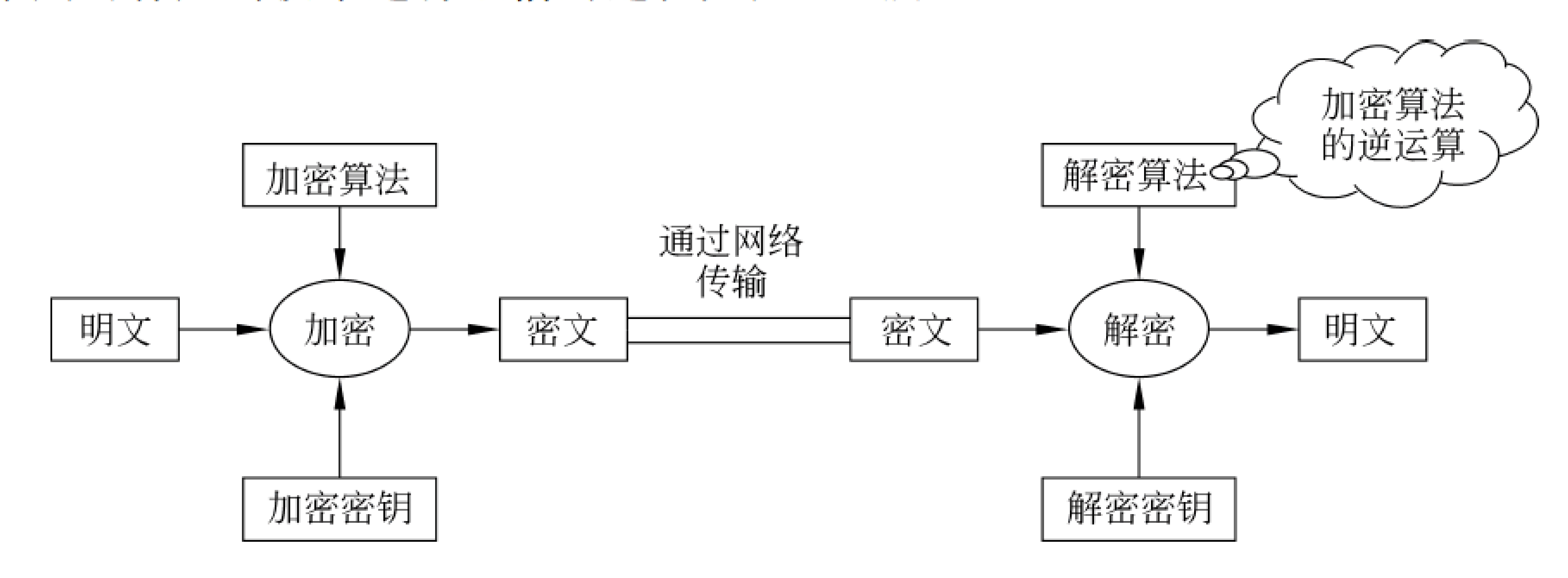
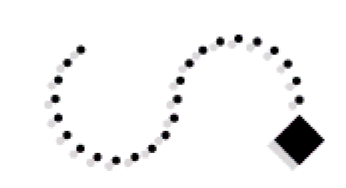


图 7-3 对称加密算法模型

1. 传统的加密技术

(1) 替换密码技术

替换密码技术将明文字母表中的每个字符替换为密文字母表中的字符,以达到隐藏明文的目的。发送者将明文中的每一个字符按照一定的规律替换成密文中的另外一个字



符。接收者对接收到的密文进行逆替换得到明文。下面介绍两种常用的替换密码算法：单表替换密码和多表替换密码。

① 单表替换技术。

如果在替换的过程中明文的一个字符用固定的一个密文字符代替，就称为单表替换技术。最古老的单表替换密码大约出现在公元前 50 年，是由罗马皇帝朱利叶·恺撒发明的一种用于战时秘密通信的方法，这种被称为恺撒密码的技术将字母按字母表的顺序排列，并将最后一个字母和第一个字母连起来构成一个循环字母表序列，明文中的每个字母用该序列中在它后面的第三个字母来代替，由此形成密文。这种密码也称为循环移位密码，如表 7-1 所示。

表 7-1　恺撒密码中 26 个英文字母映射表

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m
密文字母	D	E	F	G	H	I	J	K	L	M	N	O	P
明文字母	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

这种映射关系可以用以下函数来表示：

$$F(P) = (P + k) \bmod n$$

式中，P 表示明文字母；n 表示字符集中的字母个数；k 表示密钥。

例如，明文 P=HOW ARE YOU，k=3，则有

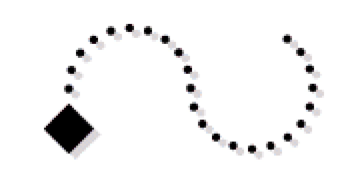
```
F(H)= (8+3)mod 26=11=K;
F(O)= (15+3) mod 26=18=R;
     ⋮
F(U)= (21+3) mod 26 =24=X;
```

可以得到的密文为 KRZDUHBRX。

对于恺撒密码，解密的方法非常简单，只要依据表中的密文字母和明文字母的对应关系，从密文字母找出相应的明文字母即可。因此这种恺撒密码是很容易被破解的，最多进行 25 次尝试就可以得到破解后的明文。由此可见，这种加密算法的安全性很差。

为了提高加密算法的安全性，可以将明文字母和密文字母的映射关系复杂化，将字母表的顺序打乱，使它们之间的映射关系变成没有规律的，即将整个字母表的 26 个字母随意映射到其他字母上。这种改进后的单表加密算法请大家自己分析，看看是否能提高破解的难度，增加加密的安全性。

在明文中，英文字母出现的频率是有一定分布规律的，即使打乱了字母表中的顺序，仍可根据自然语言的统计特性分析得到密文和明文中的对应关系。例如，在英语中最常用的字母是 e，其次是 t，再其次是 a、o、n、i。破译这种密文的方法是先计算密文中所有字母出现的相对频率，并暂时假定出现次数最多的字母为 e，其次是 t，然后寻找如 tXe 结构最多的三字母组合，假设 tXe 是英文中经常出现的定冠词 the，则 X 即为 h。以此类推，假如 thYt 型的结构也频繁出现，则可能 Y 是 a。根据这个方法，还可找到两个形如 aZW 结



 构的频繁出现的三字母组合,其相当大的可能就是 and。根据这种假设和判断,能初步构成一个试探性明文。

因此,单表替换密码技术的安全性是比较低的,为防止密码被破译,必须使密文中各字母出现的频率趋于平均,如果采用多表替换的密码技术,由于明文中的同一个字符在密文中可以表现为多种字符,所以在密文中消除了明文字母出现频率的规律,大大提高了加密的安全性。

② 多表替换技术。

多表替换技术是由多个简单代替表组成的。周期替代密码是一种常用的多表替代密码,又称为维吉尼亚(Vignere)密码,这种替代密码是循环地使用有限个字母来实现替代的一种方法。若明文信息为 p1p2p3…pn,采用 m 个字母的序列 k1k2k3…km 来实现替换,那么,p1 将根据字母 k1 的特性来替换,p2 将根据字母 k2 的特性来替换,…,pn+1 又将根据字母 k1 的特性来替换,pn+2 将根据字母 k2 的特性来替换,可用函数表示为

$$f(a) = (\mathrm{p} + \mathrm{k}i)\mathrm{mod}(n)$$

其中,字母序列 k1k2k3…km 就是加密的密钥。

这种加密技术的加密表是以字母表移位为基础把 26 个英文字母进行循环移位的,排列在一起,形成 26×26 的方阵,该方阵被称为维吉尼亚表。实际应用时,往往把某个容易记忆的词组当作密钥。维吉尼亚表见表 7-2。

表 7-2 维吉尼亚表

列 行	ABCDEFGHIJKLMNOPQRSTUVWXYZ	列 行	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A	ABCDEFGHIJKLMNOPQRSTUVWXYZ	N	NOPQRSTUVWXYZABCDEFGHIJKLM
B	BCDEFGHIJKLMNOPQRSTUVWXYZA	O	OPQRSTUVWXYZABCDEFGHIJKLMN
C	CDEFGHIJKLMNOPQRSTUVWXYZAB	P	PQRSTUVWXYZABCDEFGHIJKLMNO
D	DEFGHIJKLMNOPQRSTUVWXYZABC	Q	QRSTUVWXYZABCDEFGHIJKLMNOP
E	EFGHIJKLMNOPQRSTUVWXYZABCD	R	RSTUVWXYZABCDEFGHIJKLMNOPQ
F	FGHIJKLMNOPQRSTUVWXYZABCDE	S	STUVWXYZABCDEFGHIJKLMNOPQR
G	GHIJKLMNOPQRSTUVWXYZABCDEF	T	TUVWXYZABCDEFGHIJKLMNOPQRS
H	HIJKLMNOPQRSTUVWXYZABCDEFG	U	UVWXYZABCDEFGHIJKLMNOPQRST
I	IJKLMNOPQRSTUVWXYZABCDEFGH	V	VWXYZABCDEFGHIJKLMNOPQRSTU
J	JKLMNOPQRSTUVWXYZABCDEFGHI	W	WXYZABCDEFGHIJKLMNOPQRSTUV
K	KLMNOPQRSTUVWXYZABCDEFGHIJ	S	XYZABCDEFGHIJKLMNOPQRSTUVW
L	LMNOPQRSTUVWXYZABCDEFGHIJK	Y	YZABCDEFGHIJKLMNOPQRSTUVWS
M	MNOPQRSTUVWXYZABCDEFGHIJKL	Z	ZABCDEFGHIJKLMNOPQRSTUVWSY

例如,使用维吉尼亚密码加密明文 HOW ARE YOU,使用的密钥为 KEY,加密过程如下:给一个信息加密时,只要把密钥反复写在明文下面,每个明文字母下面对应的密钥



字母就说明该明文字母应该用维吉尼亚表的哪一行进行加密。

明文：HOW ARE YOU

密钥：KEY KEY KEY

密文：RSU KVC ISS

解密时，以密钥字母选择哪一行，从这一行中找到密文字母，那么密文字母所在的列对应的就是明文字母了。

多表替换密码技术解决了单表替换密码技术中的不安全性。对于同一个明文字母，由于对应的密钥字母不同，将得到不同的密文字母，这样就在密文中消除了明文字母出现频率的规律了。但多表替换密码也不是万无一失的，只要密码分析员拥有足够数量的密文样本，这个算法就是可以破译的，通常可以通过增加密钥的长度来增加破译的难度。

(2) 置换密码技术

置换密码技术是通过替换明文中的字母来达到隐藏真实信息的目的的。换位密码技术是通过改变明文字母的排列次序来达到加密的目的的，它把明文中的字母重新排列，字母本身不变，但位置变了。例如：把明文中的字母顺序倒过来写，然后以固定长度的字母组发送或记录。

明文：HOW ARE YOU

密文：UOY ERA WOH

最常用的换位密码是列换位密码。下面来详细说明列换位密码的工作原理。列换位加密算法中，将明文按行排列到一个矩阵中（矩阵的列数等于密钥字母的个数，行数以够用为准，如果最后一行不全，可以用不常使用的字符如 X 等填满），然后再按照密钥各个字母大小的顺序排出列号，以列的顺序将矩阵中的字母读出，就构成了密文。

密钥：4312567

明文：CAN YOU UNDERSTAND

上述明文的列换位加密算法演示如表 7-3 所示。

表 7-3　列换位加密算法演示

密　钥	4	3	1	2	5	6	7
明　文	C	A	N	Y	O	U	U
	N	D	E	R	S	T	A
	N	D	X	X	X	X	X

由上面的表格可知，按照密钥 4312567 的列顺序，按列写出该矩阵中的字母。先从第一列中得到 NEX，从第二列中得到 YRX，以此类推，得到的密文为 NEXYRXADDCNNOSXUTXUAX。

纯置换密码易于识别，因为它具有与原明文相同的字母频率。对于刚才显示的列变换的类型，密码分析相当直接，将这些密文排列在一个矩阵中，并依次改变行的位置。双字母组和三字母组频率表能够派上用场。

通过执行多次置换，置换密码的安全性能够有较大的改观，其结果是使用更为复杂的

排列，它不容易被重构。因此，如果前述消息使用相同的算法重加密，则如表7-4所示。

表7-4 二次列换位加密算法演示

密 钥	4	3	1	2	5	6	7
明 文	N	E	X	Y	R	X	A
	D	D	C	N	N	O	S
	X	U	T	X	U	A	X

密文：XCTYNXEDUNDXRNUXOAASX

为了观察这种双重置换的结果，用原明文消息中的字母所在的位置来指定该字母。在该消息中有21个字母CAN YOU UNDERSTANDXXXXX，传输的字母顺序是

01 02 03 04 05 06 07

08 09 10 11 12 13 14

15 16 17 18 19 20 21

在进行第一次置换后，得到NEXYRXADDCNNOSXUTXUAX。

03 10 17 04 11 18 02

09 16 01 08 15 05 12

19 06 13 20 07 14 21

它仍有某些规律的结构。但在第二次变换后，得到XCTYNXEDUNDXRNUXOAASX。

17 04 10 03 11 18 02

01 08 16 09 15 05 12

13 20 06 19 07 14 21

此时结构性的排列少得多，密码分析也难得多。

2. 现代对称加密算法DES

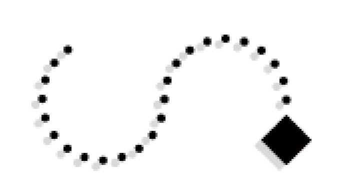
(1) DES算法及其基本原理

传统的加密方法都要求加密算法和密钥严格保密，这不利于用计算机来实现对信息的加密，因为对每个加密算法都需要编写处理程序，并且该程序必须保密，为此提出了数据加密处理算法标准化的问题。

数据加密标准(Data Encryption Standard，DES)是美国国家标准局研究的除国防部以外的其他部门的计算机系统的数据加密标准。虽然从DES出现后又产生了许多加密算法，但DES仍然是对称加密算法中最广泛使用和流行的一种加密算法。

与传统的密码技术相比，它们的基本原理一样，其密钥是保密的，但加密算法是可以公开的。传统的技术一般采用简单的算法并依靠长密钥，而现代的加密技术其密码算法十分复杂，即使破译者得到算法，没有密钥也几乎不能破译。

DES是一个分组加密算法，采用两种基本加密组块替代和换位这些技术，通过反复依次应用来提高加密算法的安全性，经过总共16轮的替代和换位后，使密码分析者无法获得该算法的一般特性以外更多的信息。



DES以64位数据为分组单位对数据加密，64位一组的明文从算法的一端输入，64位的密文从另一端输出。DES是一个对称算法，加密和解密用的是同一算法(除密钥编排的顺序不同以外)。密钥的长度为56位，密钥通常为64位的数，但每个第8位都用作奇偶校验，可以忽略。密钥可以是任意的56位的数，且可在任意的时候改变。

DES加密算法如图7-4所示，64位数据经初始变换后被置换。64位密钥去掉其第8、第16、第24、…、第64位后压缩至56位(去掉的那些位被视为奇偶校验位，不含密钥信息)，然后就开始各轮运算。64位数据经过初始置换后被分为左、右各32位两部分。56位的密钥经过左移若干位和置换后取出48位密钥子集供不同的加密迭代使用，用作加密的密钥子集记为$K(1)$、$K(2)$、…、$K(16)$。

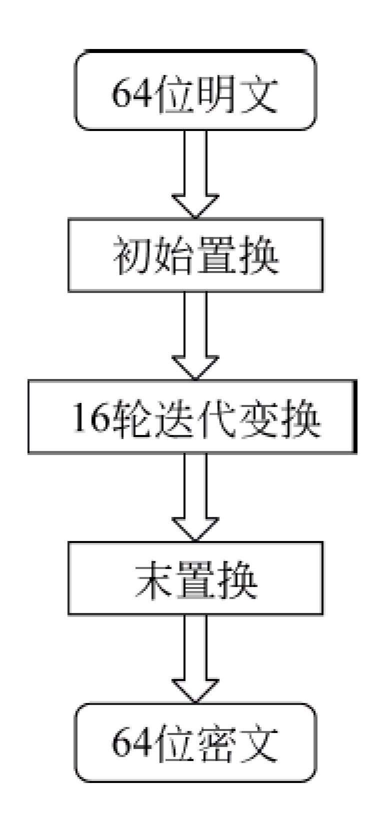


图7-4　DES加密算法

在每一轮迭代过程中，先通过重复某些位将32位的右半部分数据扩展为48位，然后密钥子集中的一个子密钥$K(i)$与数据的右半部分进行异或运算，得到的48位的结果通过S盒压缩为32位。再与数据左半部分的32位异或，其结果作为这一轮迭代的输出数据的右半部分；结合之前的右半部分作为这一轮迭代的输出数据的左半部分。这一轮输出的64位数据结果作为下一轮的待加密数据，这种迭代要重复16次。但最后一轮加密迭代之后，进行逆初始置换运算，它是初始置换的逆运算，最后得到64位密文。

(2) DES解密

DES算法的解密算法与加密算法可使用相同的算法，两者唯一的不同之处是密钥的次序相反。如果各轮加密密钥分别是$K1$、$K2$、$K3$、…、$K16$，那么解密密钥就是$K16$、$K15$、$K14$、…、$K1$。各轮产生密钥的算法也是循环的。

(3) DES算法的安全性分析

DES算法是公开的，其安全性完全取决于密钥的安全性。在该算法中，由于经过了16轮的代替、置换、异或和循环移动后，密码分析者无法通过密文获得该算法的一般特性以外的更多信息。对于这种算法，唯一的破解办法是尝试所有可能的密钥。对于56位长度的密钥，可能的组合达到$2^{56}=7.2\times10^{16}$种，用穷举法来确定某一个密钥的机会是很小的。

可见，对于DES算法的破解是比较困难的。为了更进一步提高DES算法的安全性，可以采用加长密钥的方法。例如IDEA(International Data Encryption Algorithm)算法将密钥的长度加大到128位，每次对64位的数据组块进行加密，提高了算法的安全性。

7.2.3　非对称加密技术

在对称加密算法中，加密算法简单，加密速度快，密钥简短，破解起来比较困难。但是，由于对称加密算法的安全性完全依赖于密钥的保密性，在公开的计算机网络上传送和保管密钥就成为一个严峻的问题。从传统密码出现一直到现代密码学，几乎所有的密码编码系统都建立在基本的替代和置换工具的基础上。

公开密钥密码编码学则与以前的所有方法都截然不同。一方面，公开密钥算法基于数学函数而不是替代和置换；另一方面，更重要的是，公开密钥密码编码学是非对称的，它使用两个不同的密钥，而对称的常规加密则只使用一个密钥。

非对称加密技术，也就是公开密钥算法很好地解决了传送和保管密钥这个问题。它的加密密钥和解密密钥完全不同，不能通过加密密钥推算出解密密钥。之所以称为公开密钥算法，是因为其公开密钥(Public Key)，简称公钥是公开的，任何人都能通过查找相应的公开文档得到，用它对明文加密，而另一个密钥是私有密钥(Private Key)，也称为私钥，是需要保密的，只有得到相应的私有密钥才能解密信息。

1. 公开密钥系统的原理

我们知道常规加密的密钥分配要求通信双方已经共享了一个密钥，这个密钥已经以某种方式分配给他们；或者要用一个密钥分配中心。

公开密钥算法用一个公开密钥进行加密，而用另一个不同但相关的私有密钥进行解密。仅仅知道密码算法和公开密钥而要确定私有密钥，在计算机上是不可能完成的。另外，RSA 算法还具有下列特性：两个相关密钥中的任何一个都可以用作加密而让另外一个用作解密。

公开密钥加密过程的重要步骤如下：

(1) 网络中的每个用户都产生一对用于加密和解密的密钥，即公钥和私钥。

(2) 每个用户都把自己的公钥放进一个登记本或者文件来公布它，另一个密钥需要自己妥善保存，不能让第二个用户知道。

(3) 如果 A 想给 B 发送一个报文，他就用 B 的公开密钥加密这个报文。

(4) B 收到这个报文后就用自己的私有密钥解密报文，其他所有收到这个报文的人都无法解密它，因为只有 B 才有 B 的私有密钥。

公开密钥算法示意图如图 7-5 所示。使用这种方法，所有用户都可以获得所有其他用户的公开密钥，而各用户的私有密钥由各用户在本地产生，因此不需要在网络上传送分配。只要能保密各自的私有密钥，收到的通信内容就是安全的。在任何时候，用户都可以更改他的私有密钥并公开相应的公开密钥来替代它原来的公开密钥。

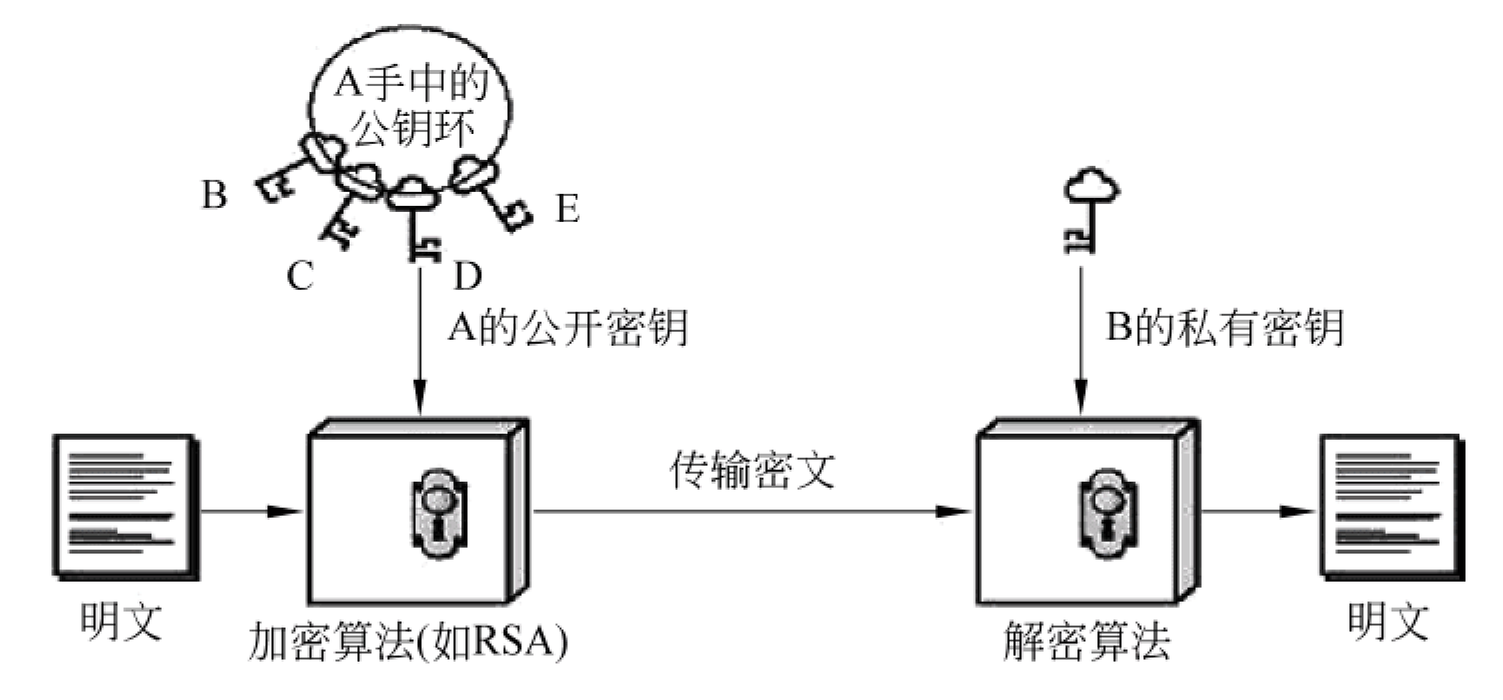


图 7-5　公开密钥算法示意图

对称加密算法和非对称加密算法的比较见表 7-5。

表 7-5　对称加密算法和非对称加密算法的比较

对 称 加 密	非对称加密
运行条件： (1) 加密和解密使用同一个密钥和同一个算法 (2) 发送方和接收方必须共享密钥和算法	运行条件： (1) 用同一个算法进行加密和解密，而密钥有一对，其中一个用于加密，另一个用于解密 (2) 发送方和接收方每一方拥有一对相互匹配的密钥中的一个
安全条件： (1) 密钥必须保密 (2) 如果不掌握其他信息，要想解密报文是不可能或者至少是不现实的 (3) 知道所用的算法加上密文的样本必须不足以确定密钥	安全条件： (1) 两个密钥中的私钥必须保密 (2) 如果不掌握其他信息，要想解密报文是不可能或者至少是不现实的 (3) 知道所用的算法，加上一个密钥，再加上密文的样本必须不足以确定另一个密钥

2. RSA 算法及其基本思想

RSA 算法是在 1977 年由美国麻省理工学院的 Ron Rivest，Adi Shamir 和 Len Adleman 三位教授研制并于 1978 年首次发表的一种算法，算法的名字取自三位教授的名字。RSA 算法是第一个公开密钥算法，是至今为止最完善的公开密钥算法之一。

RSA 是一种分组密码，其中的明文和密文都是从 0 到 $n-1$ 之间的整数。下面通过具体的例子说明 RSA 算法中密钥生成的过程。

(1) 用户 A 秘密选择两个大素数(只能被 1 和自己本身整除的整数)，为了计算方便，假设选择素数 $p=7$ 和 $q=17$。

(2) 计算 $n=p\times q=7\times 17=119$。

(3) 计算出 n 的欧拉函数 $\phi(n)=(p-1)\times(q-1)=6\times 16=96$。

(4) 选择一个 e，它小于 $\phi(n)$ 且与 $\phi(n)=96$ 互素。这样的数非常多，这里取 $e=5$。

(5) 求出 d，使得 $(d\times e)\bmod\phi(n)=1$，即 $(d\times 5)\bmod 96=1$，可得到 $d=77$。

结果用户 A 得到的公开密钥为 $\{e,n\}$，即 $\{5,119\}$；私有密钥为 $\{d,n\}$，即 $\{77,119\}$。用户 A 得到公开密钥和私有密钥后，把公开密钥告诉用户 B，用户 B 用用户 A 的公开密钥对发送的信息进行加密，然后发送给用户 A。用户 A 再用自己的私有密钥对信息进行解密。

例如，用户 B 要发送明文为 $M=19$ 的信息给用户 A，就要通过以下公式计算得到密文：$C=M^e \bmod n=19^5 \bmod 119=66$。

用户 B 将密文 66 发送给用户 A，用户 A 在接收到密文信息后，可以使用私钥恢复出明文：$M=C^d \bmod n=66^{77} \bmod 119=19$。

从上例中可以看出，从 p 和 q 计算 n 的过程非常简单，但从 $n=119$ 找出 $p=7$，$q=17$ 还是不太容易的。在实际应用中，p 和 q 将是非常大的素数(上百位的十进制数)，那样，通过 n 找到 p 和 q 的难度将非常大，甚至近乎不可能。RSA 算法的安全性基于大数分解的难度，其公钥是一对大素数的函数，从一个公钥和密文中恢复出明文的难度等价于分解两个大素数的乘积。

在使用公开密钥系统之前，每个参与者都必须产生一对密钥，这包括下列任务：

（1）确定两个素数 p 和 q。任何潜在的敌对方都可能知道 $n=pq$ 的值，为了防止通过穷举式方法发现 p 和 q，这些素数必须从足够大的集合中选取，并且用来找到大素数的方法必须相当有效。

（2）选择 e 或者 d 并且计算另外一个。

3. RSA 算法的安全性分析

RSA 算法的安全性取决于从 n 中分解出 p 和 q 的困难程度。因此，如果能够找出有效的因数分解方法，RSA 算法的安全性就没有保证了。密码分析学家和密码编码学家一直在寻找有效的因数分解方法来破解 RSA 算法。随着计算机硬件水平的发展，对一个数据进行 RSA 加密的速度已越来越快；对 n 进行因数分解的速度也越来越快，所花费的时间越来越短。

4. 密钥的管理

（1）公开密钥的分配

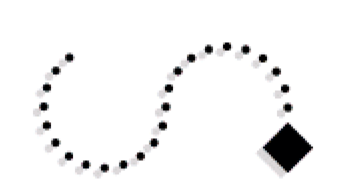
密钥管理主要处理密钥从产生到最终弃之不用的整个过程中的有关问题，包括密钥的产生、存储、导入、分配、保护、丢失和销毁等，密钥管理的主要任务就是保证在公共网络上安全传递密钥而不被窃取。非对称加密系统的一个主要应用是解决对称加密系统中对密钥的保密和分配问题。

分配公开密钥的技术方案主要有下列 4 类。

① 公开宣布：利用一个应用广泛的公开密钥加密算法，如 RSA，任何参与者都可以将消息用 RSA 算法得到的公开密钥发送给任何一个参与者，或者广播给相关人群，并将参与者的公开密钥附加在他们发送给公开论坛的报文中。这个方法虽然很方便，但存在一个致命的缺陷：任何人都可以依靠并利用这样的公开告示得到公开密钥，缺乏监督机制来约束。如用户 B 可能假装是用户 A，并发送一个公开密钥给另一个参与者 C 或者广播这样一个公开密钥，直到用户 A 发觉了伪造并警告其他参与者之前，伪造者 B 都可以阅读所有发给 A 的报文，还可以将伪造的密钥用于鉴别。

② 公开目录：通过一个可以得到的公开密钥动态目录就能够取得更大的安全性，对公开目录的维护和分配必须由一个受信任的系统或组织来负责，就像每个参与者手中都有一个公开的电话簿，自己的公开密钥都在这个目录上并可供人查询。例如，用户 A 要发送信息给用户 B，先从公开密钥的目录上查到用户 B 的公开密钥。用户 A 就可以用用户 B 的公开密钥把要发送的信息加密再发送给 B。这个方案明显比各个参与者单独进行公开告示更加安全，但是它仍然有弱点。如果一个敌对方成功地得到或者计算出了目录管理机构的私有密钥，敌对方就可以堂而皇之地散发伪造的公开密钥，并假装成任何一个参与者并窃听发送给该参与者的报文。另一个达到同样目的的方法是敌对方篡改管理机构维护的记录。

③ 公开密钥管理机构：通过更严密地控制公开密钥动态目录中的分配可以使公开密钥分配更安全。假定一个中心管理机构维护一个所有参与者的公开密钥动态目录。另外，每个参与者都知道管理机构的一个公开密钥，而只有管理机构才知道每个参与者的私



有密钥。用户 A 给公开密钥管理机构发送一个带时间戳的报文，其中包含对于 B 的当前公开密钥的请求。管理机构以一个使用它的私有密钥加密的报文进行响应，因为 A 能够使用管理机构的公开密钥解密报文，因此 A 可以确信这个报文来自管理机构，报文中包括 B 的公开密钥。A 存储 B 的公开密钥并使用它加密一个发给 B 的报文。B 可通过同样的方式得到 A 的公开密钥。A 和 B 就可以开始相互之间的秘密信息交互了。

公开密钥管理机构可能会由于大量用户请求，而使系统无法同时满足用户的要求，因为一个用户对于他所希望联系的其他用户都必须借助于管理机构才能得到公开密钥。同样，管理机构所维护的名字和公开密钥目录也可能被篡改。

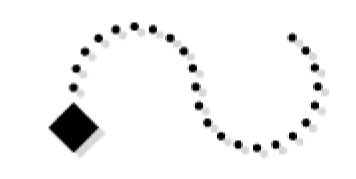
④ 公开密钥证书：采用这种方法如同直接从公开密钥管理机构得到密钥一样可靠。每个证书包含一个公开密钥以及其他信息，它由一个证书管理机构制作，并发给具有相匹配的私有密钥的参与者。一个参与者通过传输它的证书将其密钥信息传送给另一个参与者，其他参与者可以验证证书是否是管理机构制作的。每个参与者都向证书管理机构提出申请，提供一个公开密钥并请求一个证书。申请必须是面对面的或者通过某种安全的经过鉴别的方式进行。参与者可以把自己的证书发送给任何其他的参与者，接收者使用管理机构的公开密钥将证书解密，对证书进行验证。因为这个证书只能以管理机构的公开密钥进行解读，这就验证了证书的确来自证书管理机构。证书中会告诉接收者证书接收者的名字和公开密钥。最后，时间戳验证了证书的实效性。时间戳防止了参与者的私有密钥被对方获知。A 产生一个新的私有/公开密钥并向证书管理机构申请一个新的证书，而敌对方将老的证书重放给 B，如果 B 用被泄露的私有密钥对应原公开密钥加密报文，敌对方就可以解读这些报文。

私有密钥的泄露比较像信用卡丢失。持卡人挂失信用卡号码，但是在所有可能的通信方都知道旧的信用卡失效之前仍然有危险。如果一个证书过分陈旧，就可以认为它已经过期。

（2）秘密密钥的公开密钥加密分配

一旦公开密钥已经分配或者已经可以得到，就可以进行安全通信，阻止窃听、篡改或者其他的攻击行为。因为公开密钥加密的速度相对较慢，很少有用户愿意完全用公开密钥加密进行通信。因此，更合理的做法是将公开密钥加密当作一个分配常规加密所用的秘密密钥工具。

简单的秘密密钥分配过程如下：A 先产生一个私有/公开密钥对，然后给 B 传输一个报文，其中包含 A 的公开密钥和一个标识符 ID。B 产生一个秘密密钥 K，并将其用 A 的公开密钥加密后传输给 A。A 用私有密钥来恢复这个秘密密钥。A 和 B 现在就可以使用常规加密用秘密密钥进行安全通信了。信息通信完成以后，A 和 B 都丢弃这个秘密密钥 K。这种方式可以将获得密钥的危险减小到最低程度，但是这个方式容易受到主动攻击。如果一个敌对方 E 控制了中间的通信信道，结果是 A 和 B 都得到了 K，并且不知道 K 也被 E 获知。A 和 B 使用秘密密钥进行信息交互时，E 不用主动干预通信信道而只需简单地窃听。因为知道了秘密密钥，E 可以解密所有的报文，而 A 和 B 都不知道有这个漏洞存在。这种简单的协议仅仅在只存在窃听的信道环境中可以使用。



7.3 数字签名和报文鉴别

7.3.1 数字签名

身份验证服务可以确保一个通信是可信的。在诸如产生一个警告或警报信号的单个消息的情况下,鉴别服务的功能是能向接收方保证该消息发送方的真实身份。在诸如一个终端与一台主机连接这样一个正在进行的交互情况下,鉴别服务涉及两个方面。首先,在连接发起时,该服务确保这两个实体是可信的(即每个实体都的确是它们宣称的那个实体)。其次,该服务必须确保该连接不被干扰,使得第三方不能假冒这两个合法方中的任何一个来达到未授权传输或接收的目的。

在需要通过网络进行通信的环境中,会遇到以下某种攻击。

(1) 泄露:将报文内容透露给没有拥有合法密钥的任何人或相关过程。

(2) 伪装:敌方伪造一条报文却声称它源自已授权的终端。另外,还包括由假的报文接收者对收到的报文发回假确认,或者不予接收。

(3) 篡改:篡改报文的内容。

(4) 抵赖:接收者否认收到某报文或发送者否认发过某报文。

在计算机网络上进行通信时,不像书信或文件传送那样,可以通过亲笔签名或印章来确认身份。经常会发生这样的情况:发送方不承认自己发送过某一个文件;接收方伪造一份文件,声称是对方发送的;接收方对接收到的文件进行篡改,等等。那么,如何对网络上传送的文件进行身份验证呢?这就是数字签名所要解决的问题。

一个完善的数字签名应该解决好下面的三个问题。

- 当事双方因签名真伪发生争议时,应该能够在第三方或一个仲裁机构前通过验证签名来确认其真伪。
- 发送方事后不能否认自己对报文签名。
- 接收者能够验证签名,其他任何人不能伪造签名,也不能对接收或发送的信息进行篡改、伪造。

满足上述三个条件的数字签名技术,就可以解决对网络上传输的报文进行身份验证的问题了。数字签名的实现采用了密码技术,通常采用公钥加密算法实现数字签名,特别是采用RSA算法。下面,简单介绍一下数字签名的实现思想。数字签名示意图如图7-6所示。

报文进行网络传输时,发送者使用自己的私有密钥对报文信息进行加密就形成了签名。将加密的报文发送给接收者。接收者在接收到加密的报文后,采用已知发送者的公钥对报文进行解密运算,就可以核实签名。

上述过程实现了对报文信息的数字签名,但报文并没有进行加密,如果其他人截获了报文并知道了发送者的身份,就可以通过查阅文档得到发送者的公钥,从而获取报文的内容。

为了达到加密的目的,可以采用下面的模型:在将已签名的报文发送出去之前,先用

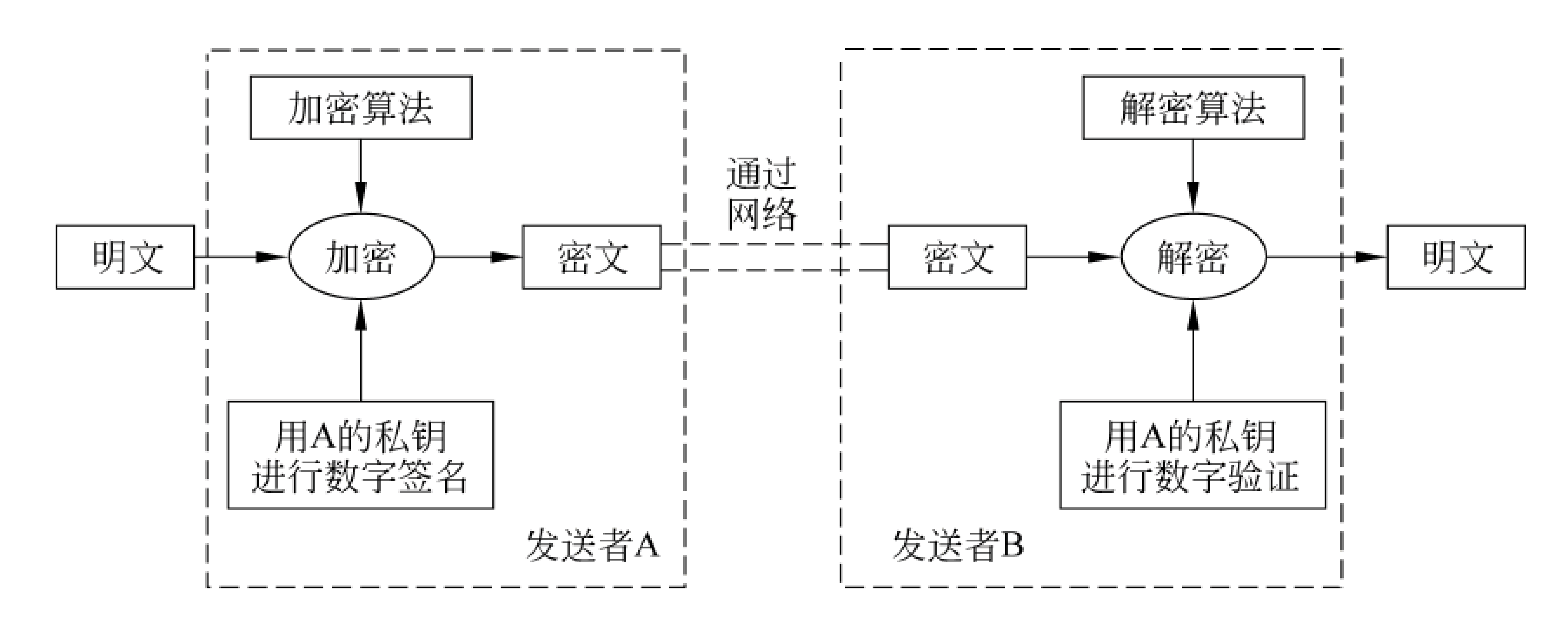


图 7-6 数字签名示意图

接收方的公钥对报文进行加密；接收方在接收到报文后先用私钥对报文进行解密，然后再用发送方的公钥验证发送方的签名。这样，就可以达到加密和签名的双重效果。

7.3.2 报文鉴别和 MD5 算法

在计算机网络安全领域中，防止信息被窃听采取的措施是对发送的信息进行加密，而防止信息被篡改和伪造需要使用报文鉴别技术。鉴别是验证通信对象是原定的发送者而不是冒名顶替的一种技术。报文鉴别保证通信的接收方能够鉴别验证所收到的报文的真伪。

报文的安全性可以通过报文加密来实现。在特定的网络应用中，许多报文并不需要加密，但是要求发送的报文是完整的、没有被篡改和非伪造的。例如，在网络上发布一个公告，就不需要加密，而只要保证其是完整的，没有被篡改。对于不需要保密的报文进行加密和解密，将会浪费计算机的系统资源并增加运算时间。因此，可使用相对简单的报文鉴别算法来达到目的。

目前，大多使用报文摘要（Message Digest，MD）算法来进行报文鉴别，其主要原理如图 7-7 所示。

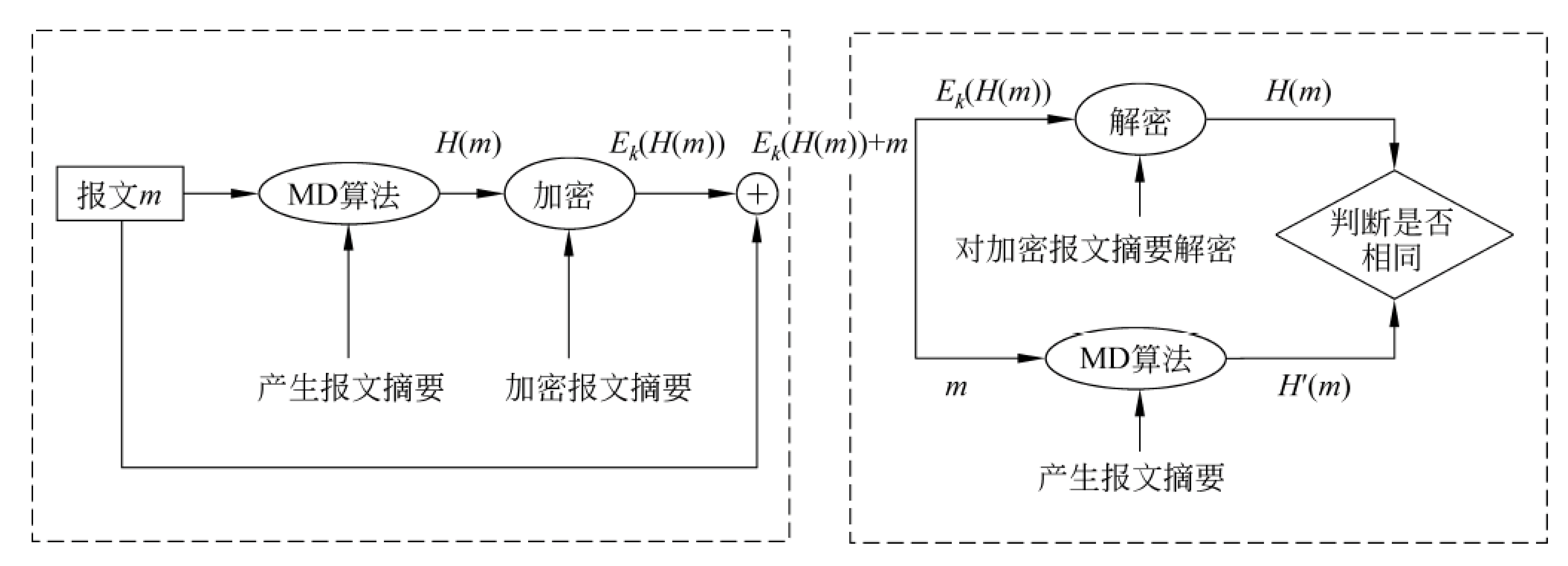


图 7-7 报文摘要原理示意图

报文摘要原理示意图说明如下：

- 发送方将待发送的可变长报文 m 经过 MD 算法运算得出固定长度的报文摘要

$H(m)$。

- 使用密钥 K 对 $H(m)$ 生成报文摘要密文 $E_k(H(m))$ 附加在报文 m 之后一起发送。
- 在接收方收到报文 m 和报文摘要密文 $E_k(H(m))$ 之后，将报文摘要密文 $E_k(H(m))$ 解密还原成 $H(m)$。
- 同时接收方将收到的报文 m 经过 MD 算法运算得出的报文摘要与 $H(m)$ 比较是否相同，若不相同则可断定收到的报文不是发送方产生的。

报文摘要的优点是：对短的固定长度的报文摘要 $H(m)$ 进行加密比对整个报文 m 进行加密的计算效率要高得多。

要实现报文 m 和加密的报文摘要 $E_k(H(m))$ 在一起是不可篡改和伪造的，是可鉴别和不可抵赖的。MD 算法必须满足两个条件。

(1) 对于给定的一个报文摘要值 x，若想找到一个报文 y，使得 $H(y)=x$ 在计算上不可行，或者想从算法上得到结果，其时间代价之高是无法承受的；

(2) 两个不同报文产生同样的报文摘要在计算上是不可行的。

这两个条件表明：$(m,H(m))$ 是发送方产生的报文和报文摘要，攻击者不可能仿造另一个报文 m'，使得 $H(m')=H(m)$，从而达到报文鉴别的目的。同时发送方可以对 $H(m)$ 进行数字签名，使报文成为不可抵赖的。

报文摘要一般采用散列函数(Hash Function)实现，目前用得最为广泛的是 MD5 报文摘要算法。

MD5 属于一种被称之为“报文摘要算法”的哈希函数，MD5 系统的定义是算法以一个任意长的信息作为输入，产生一个 128 位的“指纹”或“摘要信息”。MD5 系统主要用在数字签名和报文鉴别中。

MD5 算法是对需要进行摘要处理的报文信息块按 512 位并行处理的。首先将需要进行摘要处理的报文信息块进行填充，使信息报文的长度等于 512 的倍数。填充的方法是首先在需要进行摘要处理的报文信息块后填充 64 位的信息长度，其首位为 1，其他位全为 0；然后对信息报文依次处理，每次处理 512 位，每次进行 4 轮 16 步总共 64 步的信息变换处理，每次输出结果为 128 位，然后把前一次的输出作为下一次信息变换的输入初始值(第一次初始值算法已经固定)，这样最后输出一个 128 位的哈希摘要结果。目前 MD5 被认为是最安全的报文摘要算法之一，已经在很多应用中被当成标准使用。

MD5 提供了一种单向的哈希函数，是一种校验和报文鉴别工具。MD5 将一个任意长的字符串作为输入，产生一个 128 位的报文摘要，附在信息报文后面，以确保鉴别报文以防篡改。MD5 认为对两个不同报文产生同样的报文摘要在计算上是不可行的，并且一个已给定的报文摘要对另一个报文产生同样的报文摘要也是不可计算的。MD5 的散列结果为 128 位。采用穷举法攻击每秒 10 亿条明文约需要计算 10 年。

MD5 算法是对付特洛伊木马程序(有关特洛伊木马的知识将在后面的相关章节中详细介绍)的非常有效的工具。通过 MD5 算法计算每个文件的数字签名可检查文件是否被更换或是否与原来的一致。



7.4　信息安全技术在电子商务中的应用

网络在人们日常生活和工作中的应用越来越广泛，作为 21 世纪的主要经济形式——电子商务，将给全世界的经济带来巨大的变革。电子商务可以大幅度降低交易成本，增加贸易机会，简化贸易流程，提高贸易效率，改善物流环节，推动企业和国民经济结构的改革。电子商务是一个机遇和挑战共存的新领域，这种挑战大多数来源于对使用的安全技术的信赖。如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，是商家和用户都十分关注的话题。安全问题已成为电子商务的核心问题。要加强电子商务的安全，需要企业本身采取更为严格的管理措施，需要国家建立健全的法律制度，更需要科学的、先进的安全技术。

7.4.1　电子商务的安全概述

当今世界上最著名的阿里巴巴网站是全球最大的网上贸易市场和商人社区，为来自 220 多个国家和地区的 760 多万企业和商人提供网上商务服务。很多中小企业通过电子商务获得了巨大商机，但也有些企业由于网上交易陷入欺诈陷阱。所以要充分认识到电子商务为企业带来的益处，但同时也要看到电子商务目前发展的不完善。

1. 电子商务的基本结构和流程

目前世界上通过 Internet 进行电子商务的个人和企业不断增加，但如果把信用卡的号码、有效期限、使用者姓名等重要信息直接通过网络传送，每个人都会有所担心，会不会泄露我的信息，会不会有人盗用信用卡等问题。因此必须建立一个安全可靠地进行电子商务数据交换的系统。

电子商务的服务模式主要有：企业内部之间、企业和企业之间、企业与消费者之间等。企业—企业和企业—消费者的电子商务交易过程是有差异的，和传统的商务活动不同的是，在电子商务的流程中，企业、消费者、银行和第三方交易平台、认证体系、物流配送体系等积极参与交易的整个过程。虽然电子商务的发展是不可阻挡的潮流，但是目前在发展过程中还面临一些基本问题，也称为电子商务发展过程中的七大瓶颈，它们分别是认证体系、安全保障、在线支付安全、物流配送体系、互联网络的带宽、法律环境以及协同作业平台问题。企业在实施电子商务时必须正视这些问题，并协同寻求解决之道。

传统企业要根据电子商务的发展趋势确立自己的 Internet 发展策略。通过 Internet 建立全新的商业模式，将商业行为的主导权从卖方转移到买方，使消费者拥有更全面的信息、更多的选择和更强大的交易工具，在交易中逐步占据主动地位。电子商务需要全新的商业理念。对一些企业来说，电子商务的应用，简单地使用 Web 是不够的，必须重新考虑企业的电子商务应用环境、原有的信息管理技术和业务流程。Internet 使企业能以从前不可想象的方式，将自身运作和其他组织整合在一起。

网上交易流程有很多种类型，主要分为网络商品直销和网络商品中介交易这两种基本的流程。

(1) 网络商品直销的流程

网络商品直销是指消费者和生产者或者需求方和供应方直接利用网络形式所开展的买卖活动。这种在网上的买卖交易最大的特点是供需直接见面，环节少，速度快，费用低廉。

- 消费者在 Internet 上查看企业和商家的主页(Home Page)。
- 消费者通过购物对话框填写姓名、地址、商品品种、规格、数量、价格。
- 消费者选择支付方式，如信用卡、借记卡、电子货币、电子支票等。
- 企业或商家的客户服务器接到订单后检查支付方的服务器，确认汇款额是否被认可。
- 企业或商家的客户服务器确认消费者付款后，通知销售部门送货上门。
- 消费者的开户银行将支付款项传递到信用卡公司，并由信用卡公司负责发给消费者收费单。

在上述过程中，认证中心(CA)作为第三方，确认网上经商者的真实身份，保证了交易的正常进行。

网络商品直销的诱人之处，在于它能够有效地减少交易环节，大幅度地降低交易成本，从而降低消费者所得到的商品的最终价格。消费者只需输入厂家的域名，访问厂家的主页，即可清楚地了解所需商品的品种、规格、价格等情况，而且，该商品厂家主页上的价格最接近出厂价，这样就有可能达到出厂价格和最终价格的统一，从而使厂家的销售利润大幅度提高，竞争能力不断增强。

网络商品直销的不足之处主要表现在两个方面。第一，购买者只能从网络广告上判断商品的型号、性能、样式和质量，对实物没有直接的感知，在很多情况下可能产生错误的判断；某些厂商也可能利用网络广告对自己的产品进行不实的宣传，甚至可能打出虚假广告欺骗顾客。第二，购买者利用信用卡进行网络交易，不可避免地要将自己的密码输入计算机，由于新技术的不断涌现，犯罪分子可能利用各种高新科技的作案手段窃取密码，进而盗窃用户的钱款，这种情况不论是在国外还是在国内均有发生。

(2) 网络商品中介交易的流程

网络商品中介交易是通过网络商品交易中心，即虚拟网络市场进行商品交易的，如阿里巴巴，或购物网站如易趣网等。在这种交易过程中，网络商品交易中心以 Internet 网络为基础，利用先进的通信技术和计算机软件技术，将商品供应商、采购商和银行紧密地联系起来，为客户提供市场信息、商品交易、仓储配送、货款结算等全方位的服务。

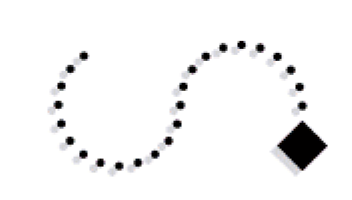
买卖双方各自的供需信息通过网络告诉网络商品交易中心，网络商品交易中心通过信息发布服务向交易的参与者提供大量的、详细准确的交易数据和市场信息。

买卖双方根据网络商品交易中心提供的信息，选择自己的贸易伙伴。网络商品交易中心从中撮合，促使买卖双方签订合同。

买方在网络商品交易中心指定的银行办理转账付款手续。

网络商品交易中心在各地的配送部门将卖方货物送交买方。

通过网络商品中介进行交易具有许多突出的优点。首先，网络商品中介为买卖双方展现了一个巨大的世界市场，这个市场存储了全世界几千万个品种的商品信息资料，可联



系千万家企业和商贸单位。每一个参加者都能够充分地宣传自己的产品，及时地沟通交易信息，最大限度地完成产品交易。各种网络商品中介机构通过网络彼此连接起来，进而形成全球性的大市场，目前这个市场正以每年 70%的速度递增。其次，网络商品交易中心作为中介方可以监督交易合同的履行情况，有效地解决在交易中买卖双方产生的各种纠纷和问题。最后，在交易的结算方式上，网络商品交易中心采用统一集中的结算模式，对结算资金实行统一管理，有效地避免了多形式、多层次的资金截留、占用和挪用，提高了资金风险防范能力。

网络商品的中介交易方式目前存在的主要问题是，现在使用的合同文本还是以买卖双方签字交换的方式完成，如何过渡到电子文本合同，并在法律上得以认可，尚需解决有关技术和法律问题。

2. 电子商务安全因素与安全技术

(1) 电子商务的安全要素

- 有效性：电子商务以电子形式取代了纸张，那么如何保证这种电子形式的贸易信息的有效性则是开展电子商务的前提。电子商务作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、确定的地点是有效的。
- 机密性：电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的的。电子商务是建立在一个较为开放的网络环境上的(尤其 Internet 是更为开放的网络)，维护商业机密是电子商务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。
- 完整性：电子商务简化了贸易过程，减少了人为的干预，同时也带来了维护贸易各方商业信息的完整、统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、重复或传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。因此，要预防信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复并保证信息传送次序的统一。
- 可靠性/不可抵赖性/鉴别：电子商务可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是交易所期望的贸易方，这一问题则是保证电子商务顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或加盖印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生，这也就是人们常说的白纸黑字。在无纸化的电子商务方式中，通过手写签名和加盖印章进行贸易方的鉴别已是不可能的了。因此，要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。
- 即需性是防止延迟或拒绝服务，即需安全威胁的目的就在于破坏正常的计算机处

理或完全拒绝服务。在电子商务中，延迟一个消息或消除它会带来灾难性的后果。例如，你在上午10点向在线的股票交易公司发一个电子邮件委托购买1000股IBM公司的股票，假如这个邮件被延迟了，股票经济商在下午2点半才收到这封邮件，这时股票已经涨了15%，这个消息的延迟就使你损失了交易额的15%。

- 身份认证：指交易双方可以相互确认彼此的真实身份，确认对方就是本次交易中所称的真正交易方。认证是证实一个声称的身份或者角色，如用户、机器、节点等是否真实的过程。这一过程是授权和审计所必需的，也是实现授权、审计的访问控制过程运行的前提，是计算机网络安全系统不可缺少的组成部分。
- 审查能力：根据机密性和完整性的要求，应对数据审查的结果进行记录。审查能力是对每个经授权的用户活动的唯一标识和监控，以便对其所使用的操作内容进行审计和跟踪，防止当贸易一方发现交易对自己不利时否认电子商务行为。

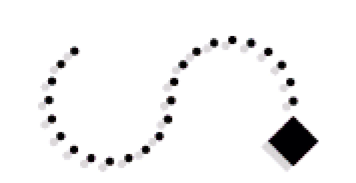
(2) 电子商务中使用的信息安全技术

为了保证电子商务交易的安全，在电子商务中使用了各种信息安全技术。

- 加密技术。加密技术是电子商务中采用的主要安全措施，交易双方可根据需要在信息交换阶段对传送的信息加密。
- 密钥管理技术。对称密钥管理是基于共同保守密钥来实现的，采用对称加密技术的双方必须保证采用安全可靠的方式来保护密钥，同时要设定防止密钥泄露和更改密钥的程序。使用公开密钥的交易双方可以使用证书来交换公开密钥。数字证书能够起到标识交易双方的作用，是目前电子商务中使用较为广泛的技术之一。
- 数字签名。数字签名是公开密钥加密技术的另一类应用，报文的发送方从报文摘要中生成一个128位的散列值，发送方用自己的私有密钥对这个散列值进行加密来形成发送方的数字签名，通过数字签名能够实现对原始报文的签名和不可抵赖性。
- 防火墙技术。防火墙主要用来隔离内部网络和外部网络，保护内部网络不受外部网络的攻击。目前防火墙主要有包过滤技术和应用网关—代理服务器。包过滤技术是指在网络层中按照过滤规则对数据包实施有选择的通过。应用网关—代理服务器可针对网络应用服务协议即数据过滤协议进行存取控制，并且能够对数据进行分析并形成相关的报告。
- CA技术。认证机构体系CA是指一些不直接从电子商务贸易中获利的受法律保护的可信任的权威机构，负责发放和管理电子证书，使网上通信的各方能互相确认身份。它的基本功能有：接收注册请求，处理、拒绝/批准请求，颁发证书。在实际运用中，CA由大家都信任的机构担当，如中国数字认证中心等。

7.4.2 电子商务中使用的安全协议

在电子商务发展中，最关键的问题是如何在开放的公开网络上保证交易的安全性，即如何构筑一个安全的交易模型问题。一个安全的电子交易模型应该包括5个方面的内容：数据保密、身份认证、数据完整性、防抵赖性、访问控制。目前，有两种安全在线支付



协议被广泛采用，即 SSL 协议和 SET 协议。

1. SSL 协议

安全套接层(Secure Socket Layer，SSL)协议是网景(Netscape)公司提出的一种基于 Web 应用的网络安全通信协议，它包括服务器认证、客户认证、SSL 链路上的数据完整性和 SSL 链路上的数据保密性，主要采用公开密钥体制和 X.509 数字证书技术来提供数据传输的安全性保证。对于电子商务应用来说，SSL 协议可保证信息的真实性、完整性和保密性。但由于 SSL 不对应用层的消息进行数字签名，因此不能提供交易的不可否认性，这是 SSL 在电子商务使用中的最大不足。因此，网景公司在从 Communicator 4.04 版开始的所有浏览器中引入了一种被称做表单签名(Form Signing)的功能，在电子商务中，可利用这一功能对包含购买者的订购信息和付款指令的表单进行数字签名，从而保证交易信息的不可否认性。SSL 协议的整个概念可以总结为：一个保证任何安装了安全套接层的客户机和服务器间事务安全的协议，它涉及所有 TCP/IP 应用程序。

(1) SSL 安全协议主要提供三方面的服务。

- 对用户和服务器进行认证，确保数据发送到正确的客户机和服务器；
- 加密数据以防止数据在传输过程中被窃取；
- 维护数据的完整性，确保数据在传输过程中不被改变。

(2) SSL 协议的工作流程。

服务器认证阶段：①客户端(即消费者)向服务器(即商家)发送一个开始信息 Hello 以便开始一个新的会话连接。②服务器根据客户端的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户端发送的 Hello 信息时将包含生成主密钥所需的信息。③客户端根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器。④服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

客户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回(数字)签名后的提问及其公开密钥，从而向服务器提供认证。

从 SSL 协议所提供的服务及其工作流程可以看出，SSL 协议运行的基础是商家对消费者信息保密的承诺，这有利于商家而不利于消费者。在电子商务初级阶段，能运作电子商务的企业大多是信誉较高的大公司，因此这个问题还没有充分暴露出来。但随着电子商务的发展，越来越多的中小型公司也参与了电子商务。

在电子支付过程中，中小型公司由于没有强制的监督机制，没有资质的公司利用电子商务在网上进行交易，这种只有商家对消费者的认证，而缺乏消费者对商家认证的单一认证问题就越来越突出。虽然在 SSL3.0 中通过数字签名和数字证书可实现浏览器和 Web 服务器双方的身份验证，但是 SSL 协议仍存在一些问题，例如，只能提供交易中客户与服务器间的双方认证，在涉及多方的电子交易中，SSL 协议并不能协调各方间的安全传输和信任关系。在这种情况下，VISA 和 MasterCard 两大信用卡公组织制定了 SET 协议，为网上信用卡支付提供了全球性的标准。

2. SET 协议

安全电子交易(Secure Electonic Transcation,SET)协议由美国 VISA 和 MasterCard 两大信用卡组织联合国际上多家科技机构，共同制定的应用于 Internet 的以银行卡为基础进行在线交易的安全标准，目的是保证网络交易的安全。SET 协议主要是为了解决信用卡在电子商务交易中的交易协议、信息保密、资料完整以及身份认证等问题。

SET 采用公钥密码体制和 X.509 数字证书标准，主要应用于企业—消费者模式中，保障网上购物信息的安全性。SET 协议本身比较复杂，设计比较严格，安全性高，它能保证信息传输的机密性、真实性、完整性和不可否认性。SET 协议是公钥基础设施(PKI)框架下的一个典型实现，同时也在不断升级和完善，如 SET2.0 将支持借记卡电子交易。

SET 协议的工作流程如下：

(1) 消费者利用自己的 PC 通过 Internet 选定所要购买的物品，并在计算机上输入订货单，订货单上需包括在线商店、购买物品名称及数量、交货时间及地点等相关信息。

(2) 通过电子商务服务器与相关在线商店联系，在线商店做出应答，告诉消费者所填订货单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。

(3) 消费者选择付款方式，确认订单签发付款指令，此时 SET 开始介入。

(4) 在 SET 中，消费者必须对订单和付款指令进行数字签名，同时利用双重签名技术保证商家看不到消费者的账号信息。

(5) 在线商店接受订单后，向消费者所在银行请求支付认可。信息通过支付网关到收单银行，再到电子货币发行公司确认。批准交易后，返回确认信息给在线商店。

(6) 在线商店发送订单确认信息给消费者。客户端软件可记录交易日志，以备将来查询。

(7) 在线商店发送货物或提供服务并通知收单银行将钱从消费者的账号转移到商店账号，或通知发卡银行请求支付。在认证操作和支付操作中间一般会有一个时间间隔，例如，在每天的下班前请求银行结一天的账。

SET 从第(3)步开始起作用，一直到第(6)步，在处理过程中通信协议、请求信息的格式、数据类型的定义等 SET 都有明确的规定。在操作的每一步，消费者、在线商店、支付网关都通过 CA(认证中心)来验证通信主体的身份，以确保通信的对方不是冒名顶替的，所以，也可以简单地认为 SET 规格充分发挥了认证中心的作用，以维护在任何开放网络上的电子商务参与者所提供信息的真实性和保密性。

由于 SET 协议提供了消费者、商家和银行之间的认证，确保了交易数据的安全性、完整性、可靠性和交易的不可否认性，特别是保证不将消费者银行卡号暴露给商家，因此 SET 成为目前公认的信用卡/借记卡网上交易的国际安全标准。

3. SET 与 SSL 协议的比较

(1) 在认证要求方面，早期的 SSL 并没有提供商家身份认证机制，虽然在 SSL3.0 中可以通过数字签名和数字证书实现浏览器和 Web 服务器双方的身份验证，但仍不能实现多方认证；相比之下，SET 的安全要求较高，所有参与 SET 交易的成员(持卡人、商家、发卡行、收单行和支付网关)都必须申请数字证书进行身份识别。

(2) 在安全性方面，SET 协议规范了整个商务活动的流程，从持卡人到商家，到支付



网关，到认证中心以及信用卡结算中心之间的信息流走向和必须采用的加密、认证都制定了严密的标准，从而最大限度地保证了商务性、服务性、协调性和集成性。而SSL只对持卡人与商店端的信息交换进行加密保护，可以看作用于传输的那部分的技术规范。从电子商务特性来看，SSL并不具备商务性、服务性、协调性和集成性。因此SET的安全性比SSL高。

(3) 在网络层协议位置方面，SSL是基于传输层的通用安全协议，而SET位于应用层，对网络上的其他各层也有涉及。

(4) 在应用领域方面，SSL主要是和Web应用一起工作的，而SET是为信用卡交易提供安全的，因此如果电子商务应用只是通过Web或电子邮件，则可以不要SET。但如果电子商务应用是一个涉及多方交易的过程，则使用SET更安全、更通用些。

SSL协议实现简单，独立于应用层协议，大部分内置于浏览器和Web服务器中，在电子交易中应用便利。但SSL是一个面向连接的协议，只能提供交易中客户与服务器间的双方认证，不能实现多方的电子交易。SET在保留对客户信用卡认证的前提下增加了对商家身份的认证，安全性进一步提高。由于两协议所处的网络层次不同，为电子商务提供的服务也不相同，因此在实践中应根据具体情况来选择独立使用或两者混合使用。

本章小结

密码技术是信息安全的核心技术，本章介绍了加密算法、密钥管理、数字签名及报文鉴别等常用技术。通过密码技术加强网络中传输数据的安全，以此来提高网络安全。要求掌握加密算法的种类、密钥分配与管理方法及数字签名的实现过程等内容，对于密码技术在电子商务中的应用要求了解即可。

本章习题

1. 简述对称性加密和非对称性加密的主要特点。
2. 简述数字签名的实现思想。
3. 简述报文摘要的主要原理。
4. 简述SET与SSL协议。

第 8 章

系统安全

【本章重点】

熟悉 Windows 在域模式下加强系统安全性的主要方法。掌握计算机病毒的工作过程及常用的反病毒技术。掌握防火墙的工作原理及体系结构。理解黑客的攻击过程及常用的攻击方法。

加强计算机网络系统的安全性，除了第 4 章介绍的加强计算机网络中传输数据的安全性之外，另外的办法就是加强计算机网络中的软件和硬件的安全性。可以从多个角度进行，如从网络体系结构的角度对各层协议的安全性进行加强；也可以从系统运行软件的角度，对各种软件的安全性进行加强；还可以针对常见的破坏活动，进行安全的防范等。在本章中仅介绍一些常用的基本技术，Windows 2003 操作系统提高安全性的主要方法、防火墙技术、防计算机病毒技术及黑客的进攻。

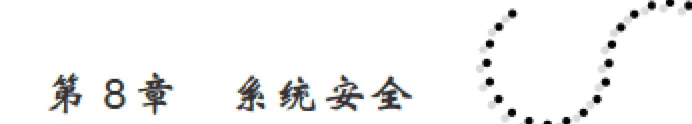
8.1 Windows 操作系统的安全性

操作系统是计算机网络系统配置最重要的软件，在整个计算机系统中处于中心地位。操作系统的安全与否，是整个计算机网络系统安全性的决定因素之一。下面就介绍 Windows 在域工作模式下提高自己安全性的主要技术。

8.1.1 Kerberos 身份认证

当网络用户对计算机网络中的资源进行访问时，系统首先进行的就是身份认证。只有被认定为合法的用户才有可能进行资源的访问。Windows 2003 在域模式下采用了 Kerberos 身份认证，保证一次登录便可进行全部访问。下面进行简单的介绍。

Kerberos 为网络通信提供可信的面向开放系统的认证服务。每当用户(client)申请得到某服务程序(server)的服务时，用户和服务程序会首先向 Kerberos 要求认证对方的身份，认证建立在用户和服务程序对 Kerberos 的信任的基础上。在申请认证时，client 和 server 都可看成 Kerberos 认证服务的用户，认证双方与 Kerberos 的关系如图 8-1 所示。



当用户登录到工作站时，Kerberos 对用户进行初始认证，通过认证的用户可以在整个登录时间内得到相应的服务。Kerberos 既不依赖用户登录的终端，也不依赖用户所请求的服务的安全机制，它本身提供了认证服务器来完成用户的认证工作。

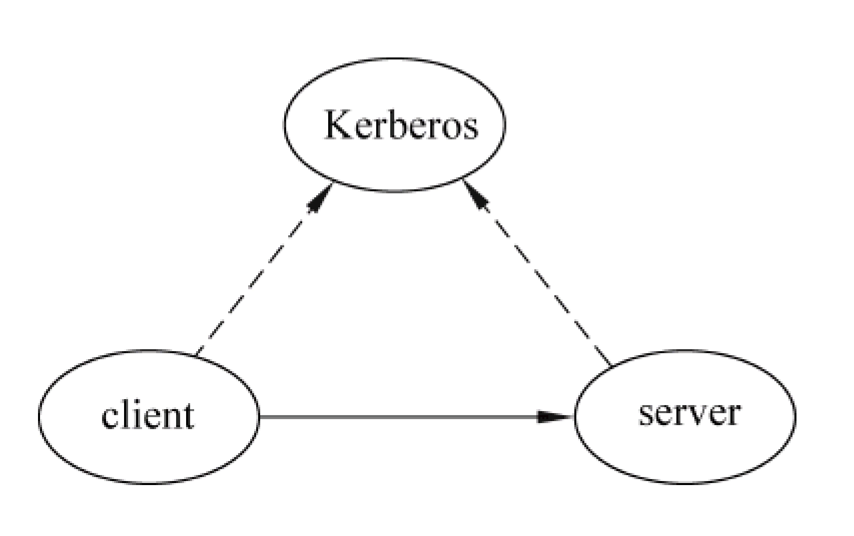


图 8-1 身份验证关系图

下面介绍一下 Kerberos 认证的过程。Kerberos 的一些常用术语的缩写如表 8-1 所示。

表 8-1 常用术语缩写

缩 写	实 际 意 义	缩 写	实 际 意 义
c	用户(client)	*K*x	x 的私有密钥
s	服务程序(server)	*K*x,y	x 和 y 的会话密钥
addr	用户的网络地址	{abc}*K*x	用 *K*x 加密 abc
Ticket	令牌，用于声明用户有效性	Tx,y	x 请求使用 y 的 Ticket
life	Ticket 保持有效的时间	Ax	x 的标识符(Authenticator)
tgs,TGS	票证服务器	WS	工作站
AS	认证服务程序		

Kerberos 有两种证书：Ticket 和 Authenticator。这两种证书均使用密钥加密，但加密的密钥不同。Ticket 用来在认证服务器和用户请求的服务之间传递用户的身份，同时也传递附加信息来保证使用 Ticket 的用户必须是 Ticket 中指定的用户。Ticket 的组成部分如图 8-2 所示。

Ticket 由 client 和 server 的名字、client 的地址、时间戳、生存时间、会话密钥 5 部分组成。Ticket 一旦生成。在 life 指定的时间内就可以被 client 多次使用来申请同一个 server 的服务。

Authenticator 则提供信息与 Ticket 中的信息进行比较，保证发出 Ticket 的用户就是 Ticket 中指定的用户。Authenticator 的组成部分如图 8-3 所示。

Tc，s={s,c,addr,timestamp,life,*K*s,c}*K*s;

图 8-2 Ticket 的组成部分

Ac={c,addr,timestamp}*K*s,c;

图 8-3 Authenticator 的组成部分

Authenticator 由 client 的名字、地址，记录当前时间的时间戳三部分组成。Authenticator 只能在一次服务请求中使用，每当 client 向 server 申请服务时，必须重新生成 Authenticator.

用户 c 请求服务 s 的整个 Kerberos 认证协议如图 8-4 所示。

(1) 用户 c 得到初始化令牌 Tc,TGS。

登录时用户被要求输入用户名，输入后系统会向认证服务器(Authentication Server)发送一条包含用户和 TGS(Ticket Granting Server)服务两者名字的请求。认证服务器

检查用户是否有效，如果有效，则随机产生一个用户用来和 TGS 通信的会话密钥 Kc，TGS，然后创建一个令牌 Tc，TGS，令牌中包含用户名、TGS 服务名、用户地址、当前时间、有效时间、还有刚才创建的会话密钥，然后将令牌用 KTGS 加密。认证服务器向用户发送加密过的令牌{Tc，TGS}KTGS 和会话密钥 Kc，TGS，发送的消息用只有用户和认证服务器知道的 Kc 来加密，Kc 的值基于用户的密码，用户与 AS 之间的数据交换，如图 8-5 所示。

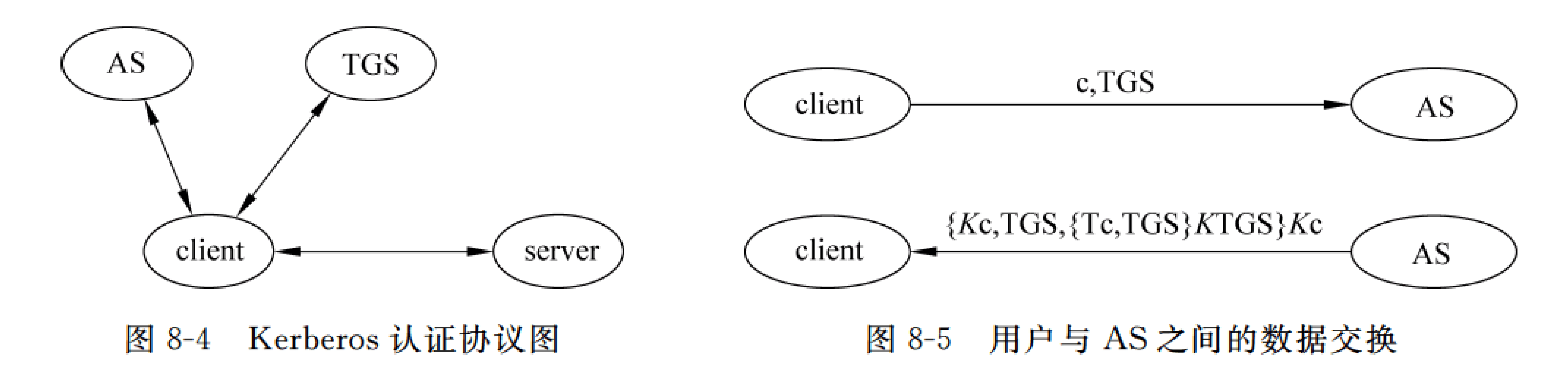


图 8-4　Kerberos 认证协议图　　　图 8-5　用户与 AS 之间的数据交换

用户工作站收到认证服务器回应后，就会要求用户输入密码，将密码转化为 DES 密钥 Kc，然后将认证服务器发回的信息解开，将令牌和会话密钥保存用于以后的通信，为了安全，用户密码和密钥 Kc 则被删掉。

当用户的登录时间超过了令牌的有效时间时，用户的请求就会失败，这时系统会要求用户使用 kinit 程序重新申请令牌 Tc，TGS。用户运行 klist 命令可以查看自己所拥有的令牌的当前状态.

（2）用户 c 从 TGS 得到所请求服务 s 的令牌 Tc，s。

一个令牌只能申请一个特定的服务，所以用户必须为每一个服务 s 申请新的令牌，用户可以从 TGS 处得到令牌 Tc，s。

用户程序首先向 TGS 发出申请令牌的请求，请求信息中包含 s 的名字、得到的请求 TGS 服务的加密令牌{Tc，TGS}KTGS，还有加密过的 Authenticator 信息{Ac}Kc，TGS，Kc，TGS 就是第(1)步得到的会话密钥。

TGS 得到请求后，用密钥和会话密钥解开请求得到的 Tc，TGS 和 Ac，根据两者的信息鉴定用户身份是否有效。如果有效，TGS 就生成用于 c 和 s 之间通信的会话密钥 Kc，s，并生成用于 c 申请得到 s 服务的令牌 Tc，s，其中包含 c 和 s 的名字、c 的网络地址、当前时间、有效时间和刚才产生的会话密钥。令牌 Tc，s 的有效时间是初始令牌 Tc，TGS 剩余的有效时间和所申请的服务默认有效时间中最短的时间，用户与 TGS 之间的数据交换如图 8-6 所示。

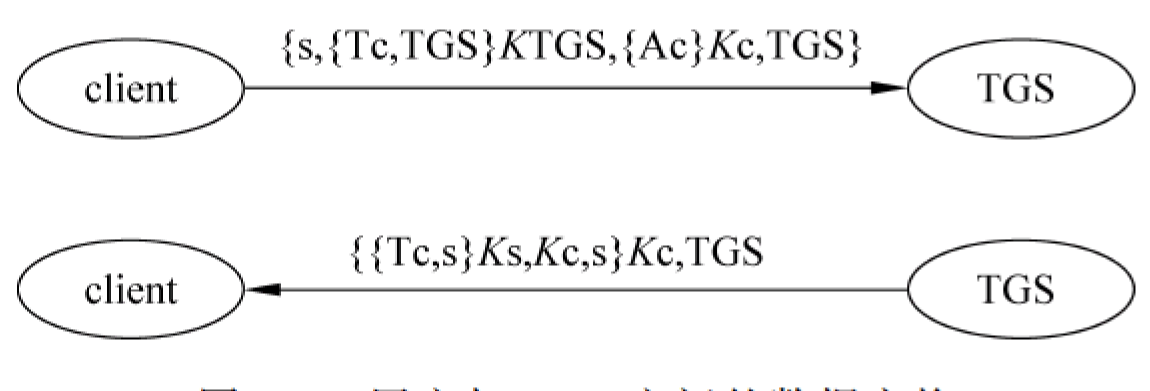
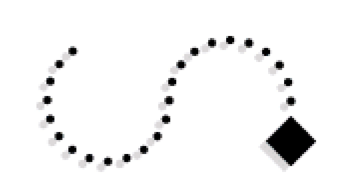


图 8-6　用户与 TGS 之间的数据交换



TGS 最后将加密后的令牌{Tc,s}*K*s 和会话密钥 *K*c,s 用用户和 TGS 之间的会话密钥加密后发送给用户。用户 c 得到回答后，用 *K*c,TGS 解密，得到所请求的令牌和会话密钥。

(3) 用户 c 利用得到的令牌 *K*c,s 申请服务 s。用户申请服务 s 的工作与第(2)步相似，只不过申请的服务由 TGS 变为了 s。

用户首先向 s 发送包含加密令牌{Tc,s}*K*s 和{Ac}*K*c,s 的请求，s 收到请求后将其分别解密，比较得到的用户名、网络地址、时间等信息，判断请求是否有效。用户和服务程序之间的时钟必须同步在几分钟的时间段内，当请求的时间与系统当前时间相差太远时，认为该请求是无效的，用来防止重放攻击。为了防止重放攻击，s 通常保存一份最近收到的有效请求的列表，当收到的请求与已经收到的某份请求的令牌和时间完全相同时，就认为此请求无效。

当 c 也想验证 s 的身份时，s 将收到的时间戳加 1，并用会话密钥加密后发送给用户，用户收到回答后，用会话密钥解密来确定 s 的身份，服务器和用户之间的数据交换如图 8-7 所示。

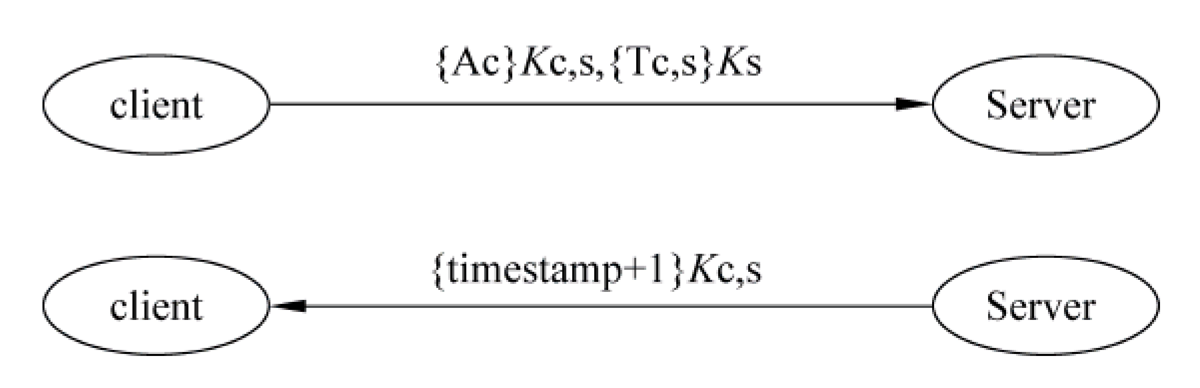


图 8-7　服务器和用户之间的数据交换

通过上面三步之后，用户 c 和服务 s 互相验证了彼此的身份，并且拥有只有 c 和 s 两者知道的会话密钥 *K*c,s，以后的通信都可以通过会话密钥得到保护。

8.1.2　访问控制

当用户成功登录系统后，用户就领到了一张身份证件，而各种资源都包含控制用户访问的控制信息，当用户试图访问资源时，系统将对比资源的访问控制信息和用户的身份证件，以确定用户是否有权访问资源，以及访问权限是什么。

1. 安全标识符

SID(Security Identifiers)是标识用户、组和计算机账户的唯一号码。在第一次创建该账户时，将给网络上的每一个账户发布一个唯一的 SID。Windows 2003 中的内部进程将引用账户的 SID 而不是账户的用户名或组名。如果创建账户，再删除账户，然后使用相同的用户名创建另一个账户，则新账户将不具有授权给前一个账户的权力或权限，原因是该账户具有不同的 SID 号。安全标识符也被称为安全 ID 或 SID。

用户通过验证后，登录进程会给用户一个访问令牌，该令牌相当于用户访问系统资源的票证，当用户访问系统资源时，将访问令牌提供给 Windows，然后 Windows 检查用户访问对象上的访问控制列表。如果用户被允许访问该对象，Windows 将会分配给用户适当的访问权限。

访问令牌是用户在通过验证的时候由登录进程提供的，所以改变用户的权限需要注销后重新登录，重新获取访问令牌。

如果存在两个同样SID的用户，这两个账户将被鉴别为同一个账户，原理上如果账户无限增加，将会产生同样的SID，在通常情况下SID是唯一的，它由计算机名、当前时间、当前用户态线程的CPU耗费时间的总和三个参数决定，以此保证它的唯一性。

一个完整的SID包括用户和组的安全描述、48位的ID标识、修订版本、可变的验证值，如s-1-5-21-76985614-1876338704-322544478-1001。

2. 访问控制

既然用户被鉴定到服务器上，就可以对照基于NTFS的任意访问控制列表(DACL)查找用户的权限。当一个用户试图访问一个文件或者文件夹的时候，NTFS文件系统会检查用户使用的账户或者账户所属的组是否在此文件或者文件夹的访问控制列表(ACL)中，如果存在则进一步检查访问控制项(ACE)，然后根据控制项中的权限来判断用户最终的权限。如果访问控制列表中不存在用户使用的账户或者账户所属的组，就拒绝用户访问。

(1) NTFS权限及对应的操作

NTFS权限及对应的操作如表8-2所示。

表8-2 NTFS权限及对应操作

权　　限	对应的操作
完全控制	对文件或者文件夹可执行所有操作
修改	可以修改、删除文件或者文件夹
读取和运行	可以读取内容，并且可以执行应用程序
列出文件夹目录	可以列出文件夹的内容，此权限只针对文件夹存在
读取	可以读取文件或者文件夹的内容
写入	可以创建文件或者文件夹
特别的权限	其他不常用的权限，如删除权限的权限

所有权限都有“允许”和“拒绝”两种选择，如图8-8所示。

关于权限的进一步说明如下。

① 新建的文件或者文件夹都有默认的NTFS权限，如果没有特别需要，一般不用改。文件或者文件夹的默认权限是继承上一级文件夹的权限，如果是根目录(如C:\)下的文件夹，则权限是继承磁盘分区的权限。权限的设置在如图8-9所示的对话框中进行。

设置各个账户以及组对当前文件或者文件夹的权限的方法很简单，在该对话框的“名称”文本框中，选择要修改的账户或者组，在“权限”列表框中选择合适的权限就行了。还可以在该对话框中设置一些特殊权限以及取得文件或文件夹的所有权的方法。

② NTFS权限的应用规则：如果一个用户同时在两个组或者多个组内，而各个组对同一个文件有不同的权限，那么这个用户对这个文件有什么权限呢？




图 8-8　NTFS 权限及对应的操作



图 8-9　权限的设置

简单地说，当一个用户属于多个组的时候，这个用户会得到各个组的累加权限，但是一旦有一个组的相应权限被拒绝，此用户的此权限就会被拒绝。

举例来说，假设有一个用户 WZ，如果 WZ 属于 A 和 B 两个组，A 组对某文件有读取权限，B 组对此文件有写入权限，WZ 自己对此文件有修改权限，那么 WZ 对此文件的最终权限为读取＋写入＋修改权限。

假设 WZ 对文件有写入权限，A 组对此文件有读取权限，但是 B 组对此文件为拒绝读取权限，那么 WZ 对此文件只有写入权限。这里还有一个小问题，WZ 对此文件只有写入权限，没有读取权限，那么，写入权限有效么？答案很明显，WZ 对此文件的写入权限无效，因为不能读取怎么写入？连门都进不去，怎么把家具搬进去？

③ 权限的继承：新建的文件或者文件夹会自动继承上一级目录或者驱动器的 NTFS 权限，但是从上一级继承下来的权限是不能直接修改的，只能在此基础上添加其他权限。也就是不能把权限上的钩去掉(因为你去不掉)，只能添加新的钩。在“属性”对话框中灰色的框为继承的权限，是不能直接修改的，白色的框是可以添加的权限。

当然这并不是绝对的，只要权限够，如管理员，也可以把这个继承下来的权限修改了，或者让文件不再继承上一级目录或者驱动器的 NTFS 权限。

④ 权限的拒绝：这个很简单，只要记住，拒绝的权限是最大的就行了。无论给账户或者组设置了什么权限，只要“拒绝”复选框被选中，被拒绝的权限就绝对有效。

⑤ 移动和复制操作对权限的影响：这里一共有 4 种情况，移动和复制文件(夹)到同一个或者不同的分区内。只需要记住，只有移动到同一分区内才能保留原来设置的权限，否则为继承目的地文件夹或者驱动器的 NTFS 权限。

(2) 共享权限

共享权限只有三种：读取、更改和完全控制。Windows Server 2008 对用户 Everyone

的默认权限是只具有读取权限，如图 8-10 所示。共享文件夹的管理者可以对共享用户进行权限指派，同时 Windows Server 2008 在共享权限的管理上提供了基于访问权限的枚举功能。



图 8-10　共享权限

下面解释一下三种权限：

- 读取权限是指派给 Everyone 组的默认权限。除此之外还能进行以下操作：查看文件名和子文件夹名、查看文件中的数据、运行程序文件。
- 更改权限不是任何组的默认权限。更改权限除允许所有的读取权限外，还增加了以下操作：添加文件和子文件夹、更改文件中的数据、删除子文件夹和文件。
- 完全控制权限是指派给本机上的 Administrators 组的默认权限，包括读取及更改权限。和 NTFS 权限一样，如果赋予某用户或者用户组拒绝的权限，则该用户或者该用户组的成员将不能执行被拒绝的操作。

对于共享文件夹应注意以下三点：

- 共享权限只对通过网络访问的用户有效，所以有时需要和 NTFS 权限配合（如果分区是 FAT/FAT32 文件系统，则不需要考虑），才能严格地控制用户的访问。当一个共享文件夹设置了共享权限和 NTFS 权限后，就要受到两种权限的控制。
- 如果希望用户能够完全控制共享文件夹，首先要在共享权限中添加此用户（组），并设置完全控制的权限。然后在 NTFS 权限设置中添加此用户（组），也设置完全控制权限。只有两个地方都设置了完全控制权限，用户（组）才最终拥有完全控制权限。
- 当用户从网络访问一个存储在 NTFS 上的共享文件夹时会受到两种权限的约束，而有效权限是最严格的权限（也就是两种权限的交集）。而当用户从本地计算机直接访问文件夹时，不受共享权限的约束，只受 NTFS 权限的约束。同时还要考虑两个权限的冲突问题，例如，共享权限为只读，NTFS 权限是写入，那么最终权限是完全拒绝，因为这两个权限的组合权限是两个权限的交集。

8.2　防火墙技术

8.2.1　什么是防火墙

防火墙就像中世纪的城堡防卫系统，那时人们为了保护城堡的安全，在城堡的周围挖了一条护城河，每一个进入城堡的人都要经过吊桥，并且还要接受城门守卫的检查。人们借鉴了这种防护思想，设计了一种网络安全防护系统，这种系统就被称为防火墙，如

图 8-11 所示。

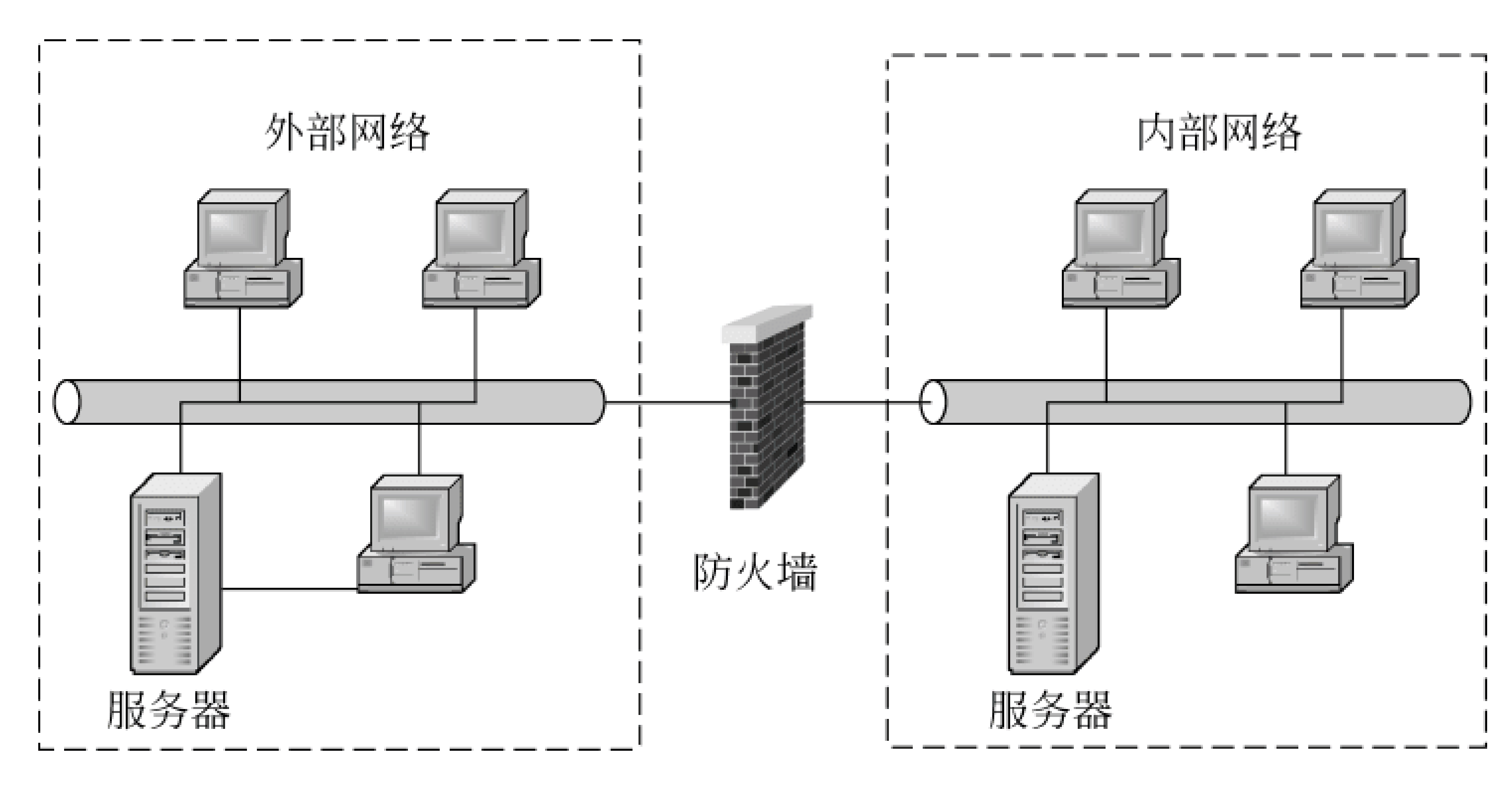


图 8-11　防火墙

计算机网络中的防火墙技术是建立在现代通信技术和信息安全技术基础上的应用性安全技术，应用于内部网络与外部网络之间，保障内部网络的安全。防火墙可以在用户的计算机和 Internet 之间建立一道屏障，把用户和外部网络隔绝；用户可以通过设定规则来决定哪些情况下防火墙应该隔绝计算机与 Internet 之间的数据传输，哪些情况下允许两者之间的数据传输。通过防火墙挡住外部网络对内部网络的攻击和入侵，从而保障用户的网络安全。

从逻辑上讲，防火墙是分离器、限制器和分析器，有效地控制了内部网络和 Internet 之间的任何活动，保证了内部网络的安全。在计算机网络中，一个网络防火墙是防备潜在的恶意活动的屏障，并可通过一个“门”来允许用户在安全网络和开放的不安全的网络之间通信。早期的防火墙是由一个单独的机器组成的，放置在私有网络和公网之间。

近年来，防火墙涉及整个从内部网络到外部网络的区域，由一系列复杂的机器和程序组成。简单地说，今天的防火墙是多个组件的应用。从实现形式上讲，防火墙可以分为硬件防火墙和软件防火墙，硬件防火墙是通过硬件和软件结合来达到隔离内部、外部网络的目的的；软件防火墙是通过纯软件的方式来实现的。

防火墙在实施安全的过程中是至关重要的。一个防火墙策略要符合 4 个目标，而每个目标通常都不是通过一个单独的设备或软件来实现的。大多数情况下防火墙的组件放在一起使用以满足公司安全目的的需求。

（1）实现一个公司的安全策略。

防火墙的主要意图是强制执行用户的安全策略。在前面的课程提到过在适当的网络安全中安全策略的重要性。举个例子，也许用户的安全策略只需对 Mail 服务器的 SMTP 流量做些限制，那么就要直接在防火墙强制这些策略。

（2）创建一个阻塞点。

防火墙在一个公司私有网络和公网间建立一个检查点，要求所有的流量都要通过这个检查点。一旦这些检查点建立，防火墙设备就可以监视、过滤和检查所有进来和出去的流量。网络安全产业称这些检查点为阻塞点。通过强制所有进出流量都通过这些检查点，网络管理员可以集中在较少的地方进行监测。如果没有这样一个供监视和控制信息的点，系

统或安全管理员就要在大量的地方进行监测。检查点的另一个名字叫做网络边界。

（3）记录 Internet 活动。

防火墙还能够强制日志记录，并且提供警报功能。通过在防火墙上实现日志服务，安全管理员可以监视所有从外部网或互联网的访问。好的日志策略是实现适当网络安全的有效工具之一。防火墙为管理员进行日志存档提供了更多的信息。

（4）限制网络暴露。

防火墙在内部网络周围创建了一个保护的边界，并且对于公网隐藏了内部系统的一些信息以增加保密性。当远程节点侦测内部网络时，它们仅仅能看到防火墙。远程设备不会知道内部网络的布局。防火墙可以通过提高认证功能和对网络加密来限制网络信息的暴露。通过对所有进来的流量进行源检查，以限制从外部发动的攻击。

防火墙的缺点主要集中在以下4点。

（1）不能防范恶意的知情者。

如果入侵者在防火墙内部，他不通过防火墙就可以删改文件，盗窃数据，破坏软件和硬件。在这种情况下防火墙是无能为力的，只能加强内部管理来防范。

（2）不能防范不通过它的连接。

如果内部网被允许不通过防火墙，而通过其他途径进行访问，那么不通过防火墙的非法访问就不能被防范。

（3）不能防备全部的威胁。

防火墙可以用来防范已知的威胁，但不能防范未知的新威胁。

（4）不能防病毒。

虽然防火墙扫描所有通过的信息，但是不能扫描数据的确切内容，即使是先进的数据包过滤也不能防范数据中隐藏的病毒。

8.2.2 防火墙的基本技术

1. 分组过滤技术

分组过滤技术是防火墙应用最基本的技术，可以用来实现多种网络安全策略。网络安全策略必须明确描述被保护的资源、服务的类型、重要程度以及防范对象。

首先在分组过滤装置的端口设置分组过滤准则（分组过滤规则），分组过滤的规则按一定的顺序存储。当一个分组到达端口时，对分组的头部进行分析，大多数分组过滤装置只检查IP、传输控制协议（TCP）、用户数据报文协议（UDP）头部内的字段，然后根据分组过滤的规则来决定是阻塞该分组还是继续发送，如果存在某条规则阻塞一个分组传递或接收，则不允许该分组通过。如果存在某条规则允许或接收一个分组，则允许该分组通过。如果一个分组不满足任何规则，则该分组被阻塞。分组过滤原理如图8-12所示。

下面根据一个简单的例子来说明分组过滤的工作原理。

有一个内部网A，它的IP地址为132.36.×.×，其中某部门的IP地址为132.36.9.×。另一个内部网B的IP地址为112.44.×.×，其中某部门的IP地址为112.44.9.×，该部门不能连接到A的内部网，允许B中其他部门的所有子网与A内部网132.36.9.×连接，但不能与A其他部门连接。过滤规则表如表8-3所示。

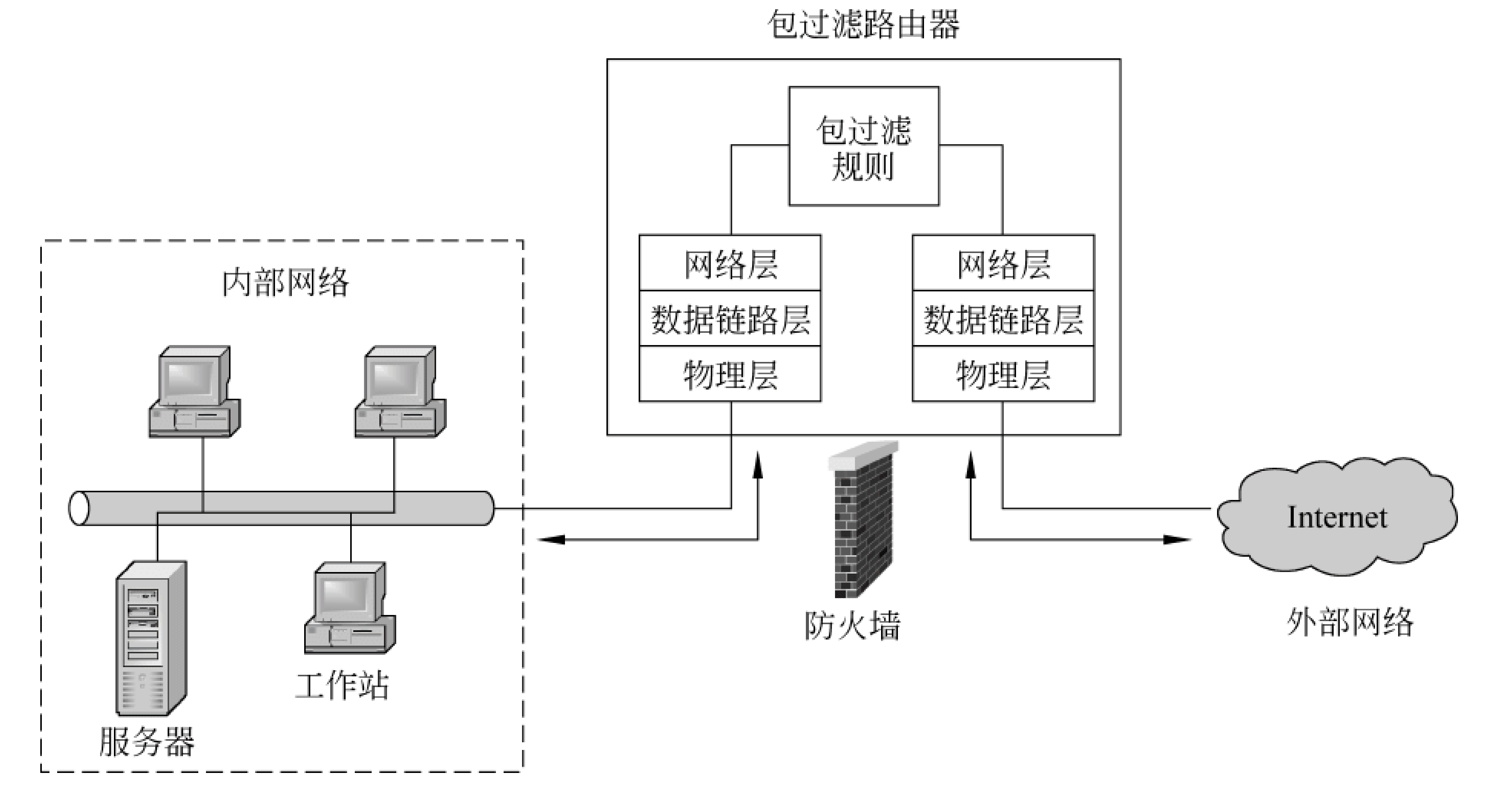


图 8-12　分组过滤原理示意图

表 8-3　过滤规则表

规则	源　地　址	目 的 地 址	动作
1	112.44.×.×	131.36.9.×	允许
2	112.44.9.×	131.36.×.×	拒绝
3	0.0.0.0	0.0.0.0	拒绝

当一个分组到达过滤端口时，分别用过滤规则表中的每条规则对分组进行检查，符合规则 1 的允许通过，符合规则 2 的将被拒绝，不允许通过。表中的规则 3 为默认值，也就是不符合规则 1 和规则 2 的其他分组将被拒绝，不允通过。

根据规则表可以得到以下结论：

对于分组 1，源地址为 112.44.9.1，目的地址为 131.36.1.1，则拒绝该分组通过。

对于分组 2，源地址为 112.44.1.1，目的地址为 131.36.9.1，则允许该分组通过。

对于分组 3，源地址为 112.24.1.1，目的地址为 131.36.1.1，则拒绝该分组通过。

一个分组过滤装置常被放置于一个或几个网段与其他网段之间。网段通常被分为内部网段和外部网段，外部网段用来连接外部网络，例如，Internet；内部网段用来连接一个单位或组织内部的主机和其他网络资源。

2. 应用程序代理技术

应用程序代理技术建立在应用层的基础上，利用应用程序来过滤 Telnet、FTP 等服务连接，这样的应用软件称为代理服务。运行代理服务的主机称为应用网关，代理服务仅允许在应用网关有代理的服务通过防火墙，而其他没有代理的服务将被阻塞。代理服务具有认证和很强的日志功能。

应用程序代理防火墙实际上并不允许在它连接的网络之间直接通信。代理服务器接受来自内部网络特定用户应用程序的通信，然后与公共网络服务器建立单独的连接。网

络内部的用户不直接与外部的服务器通信，所以服务器不能直接访问内部网的任何一部分。另外，如果不为特定的应用程序安装代理程序代码，这种服务是不会被支持的，不能建立任何连接。这种建立方式拒绝任何没有明确配置的连接，从而提供了额外的安全性和控制性。应用代理示意图如图8-13所示。

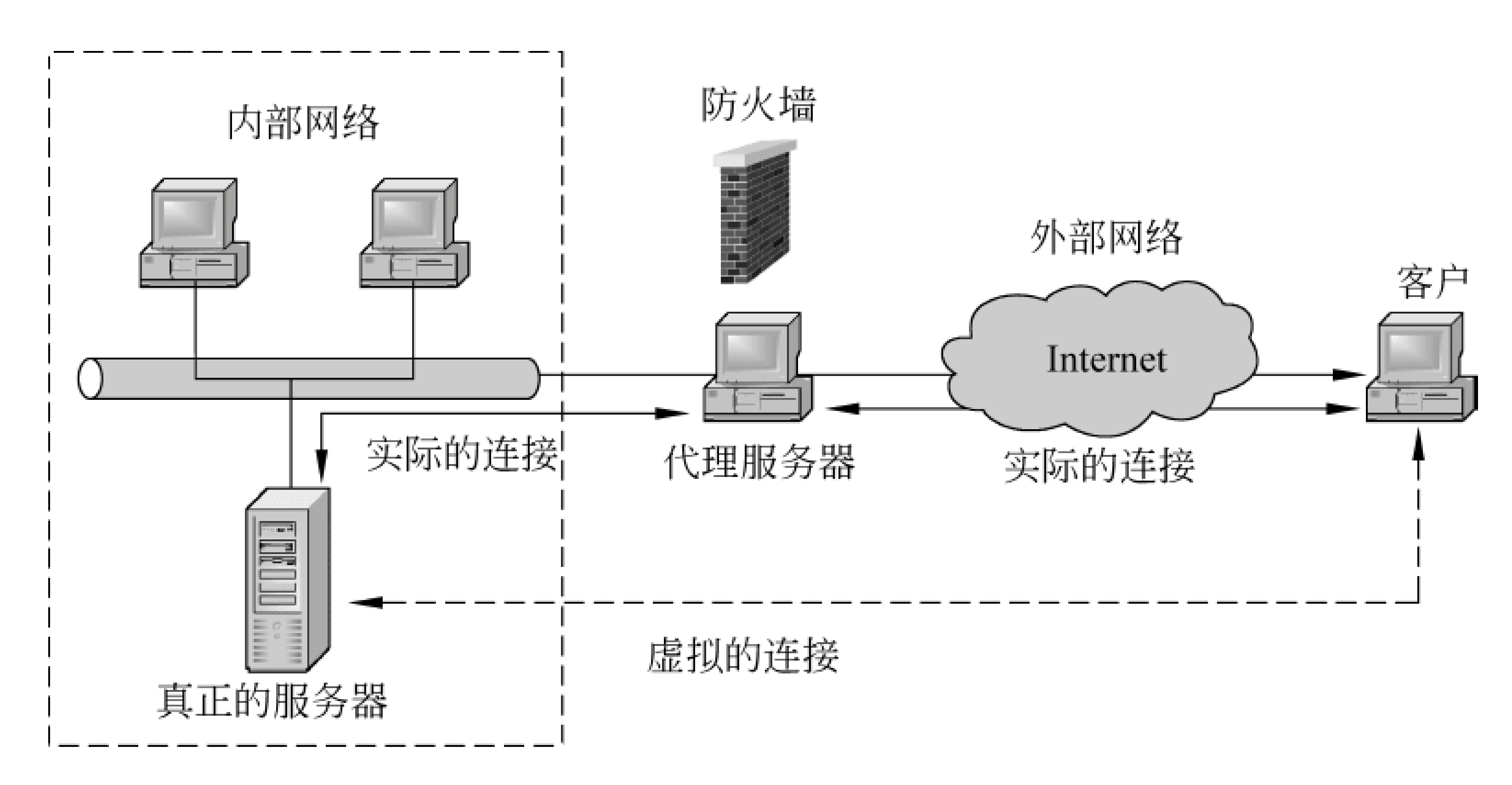


图 8-13　应用代理示意图

例如，一个用户的Web浏览器可能在80端口，但也可能在1080端口，连接到了内部网络的HTTP代理防火墙。防火墙接受这个连接请求，并把它转到所请求的Web服务器。这种连接和转移对该用户来说是透明的，因为它完全是由代理防火墙自动处理的。

代理防火墙通常支持一些常见的应用服务，如HTTP、HTTPS/SSL、SMTP/POP3、IMAP、NNTP、Telent、FTP、IRC。

应用程序代理防火墙可以配置成允许来自内部网络的任何连接，也可以配置成要求用户认证后才建立连接。要求认证的方式有只为已知的用户建立连接这种限制，为安全性提供了额外的保证。如果网络受到危害，这个功能就会使得从内部发动攻击的可能性大大减少。

3. 监测模型技术

监测模型技术根据Internet和内部网络关联的需求，建立其控制管理的模型，完成信息传输的控制与管理。从原理上讲监测模型技术对所有的协议都有效，能处理从IP层到应用层所有的分组过滤数据，也就是将所有层的信息综合到一个监测点上进行过滤。一般是加载一个检测模块，在不影响网络正常工作的前提下，检测模块在网络层截取数据包，然后在所有的通信层上抽取有关的状态信息，据此判断该通信是否符合安全策略。由于监测模型技术是在网络层截获数据包的，因此可以支持多种协议和应用程序，并可以很容易地实现应用的扩充。

8.2.3 防火墙的体系结构

最简单的防火墙配置，就是直接在内部网和外部网之间加装一个包过滤路由器或者应用网关。为更好地实现网络安全，有时还要将几种防火墙组合起来构建防火墙系统。目前比较流行的有以下三种防火墙配置方案。

1. 双宿主机网关

双宿主机网关是用一台装有两个网络适配器的双宿主机做防火墙的。双宿主机用两个网络适配器分别连接两个网络，又称为堡垒主机。堡垒主机上运行着防火墙软件(通常是代理服务器)，可以转发应用程序，提供服务等。双宿主机网关有一个致命的弱点，一旦入侵者侵入堡垒主机并使该主机只具有路由器功能，则任何网上用户均可以随便访问有保护的内部网络，如图 8-14 所示。

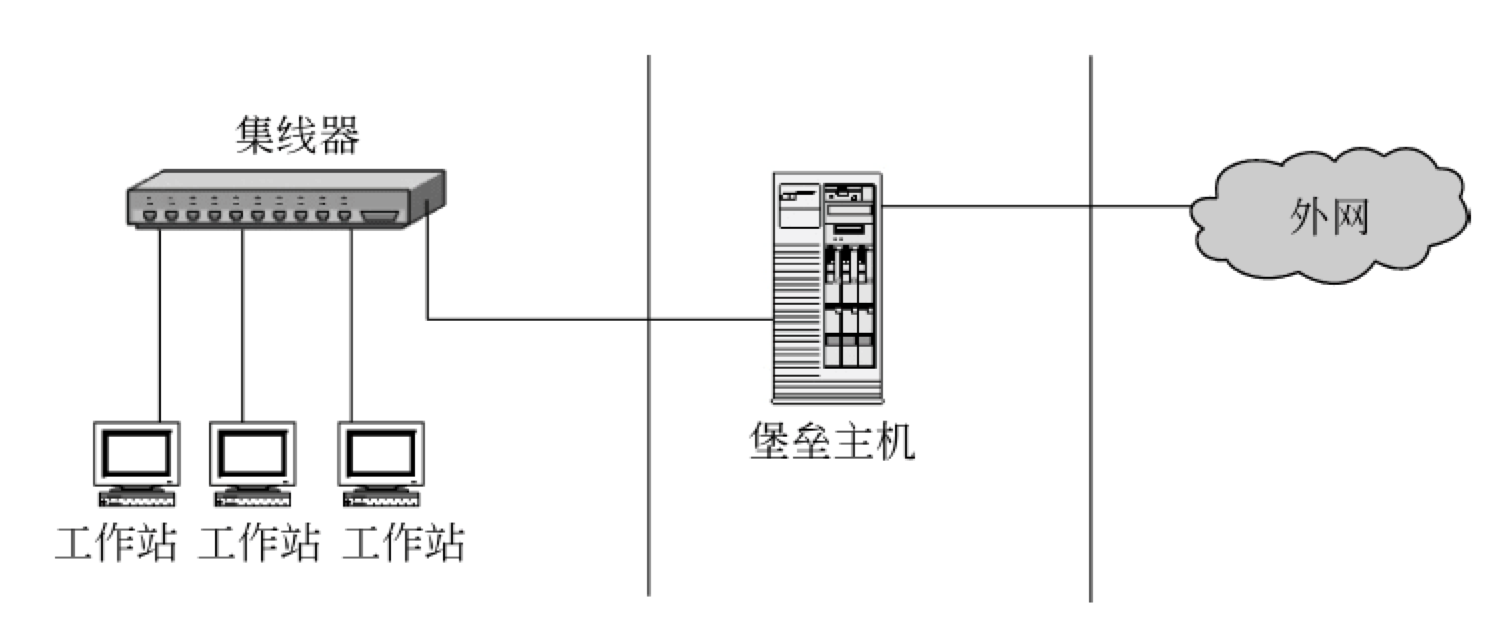


图 8-14　双宿主机网关

2. 屏蔽主机网关

屏蔽主机网关易于实现，安全性好，应用广泛。屏蔽主机又分为单宿堡垒主机和双宿堡垒主机两种类型。在单宿堡垒主机类型中，一个包过滤路由器连接外部网络，一个堡垒主机安装在内部网络上。堡垒主机只有一个网卡，与内部网络连接。通常在路由器上设置过滤规则，并使这个单宿堡垒主机成为从 Internet 上唯一可以访问的主机，确保内部网络不受未被授权的外部用户的攻击。而 Intranet 内部的客户机，可以受限制地通过屏蔽主机和路由器访问 Internet。单宿堡垒主机如图 8-15 所示。

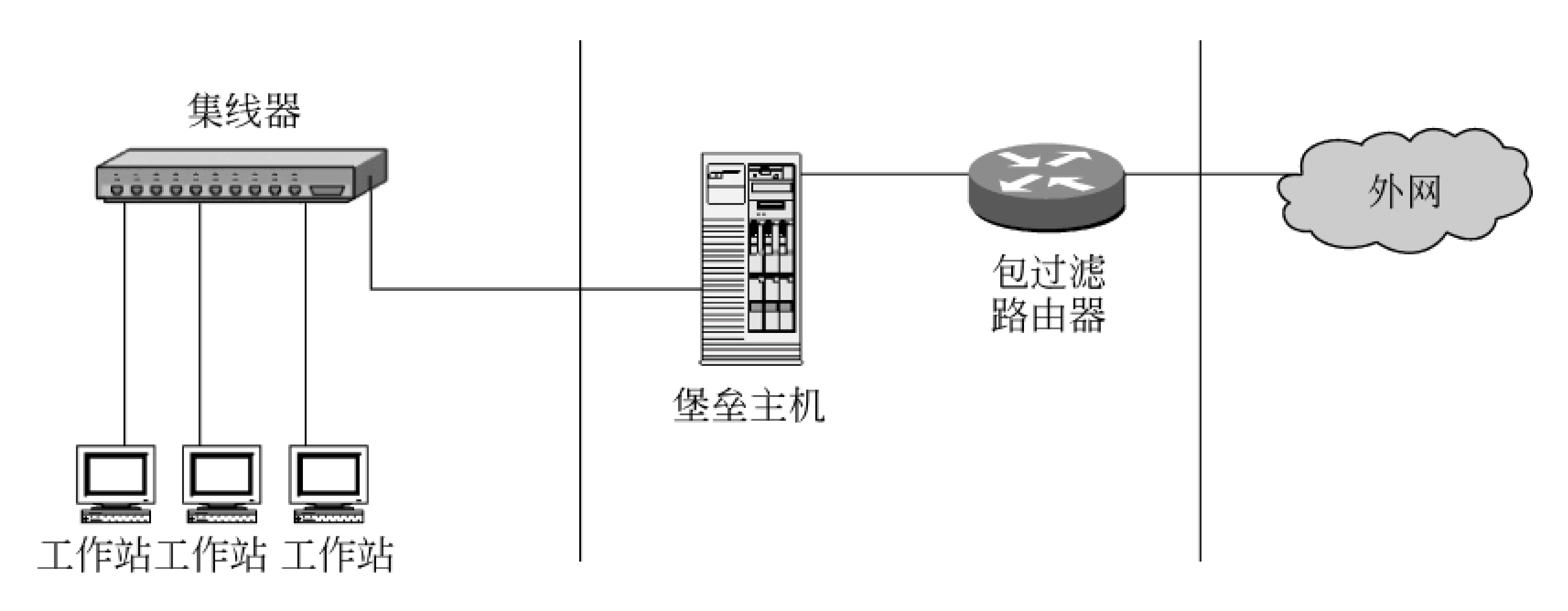


图 8-15　单宿堡垒主机

双宿堡垒主机型与单宿堡垒主机型的区别是，堡垒主机有两块网卡，一块连接内部网络，一块连接包过滤路由器。双宿堡垒主机在应用层提供代理服务，与单宿型相比更加安全。双宿堡垒主机如图 8-16 所示。

3. 屏蔽子网

屏蔽子网是在 Intranet 和 Internet 之间建立一个被隔离的子网，用两个包过滤路由器将这一子网分别与 Intranet 和 Internet 分开。两个包过滤路由器放在子网的两端，在子网内构成一个“缓冲地带”，两个路由器一个控制 Intranet 数据流，另一个控制 Internet

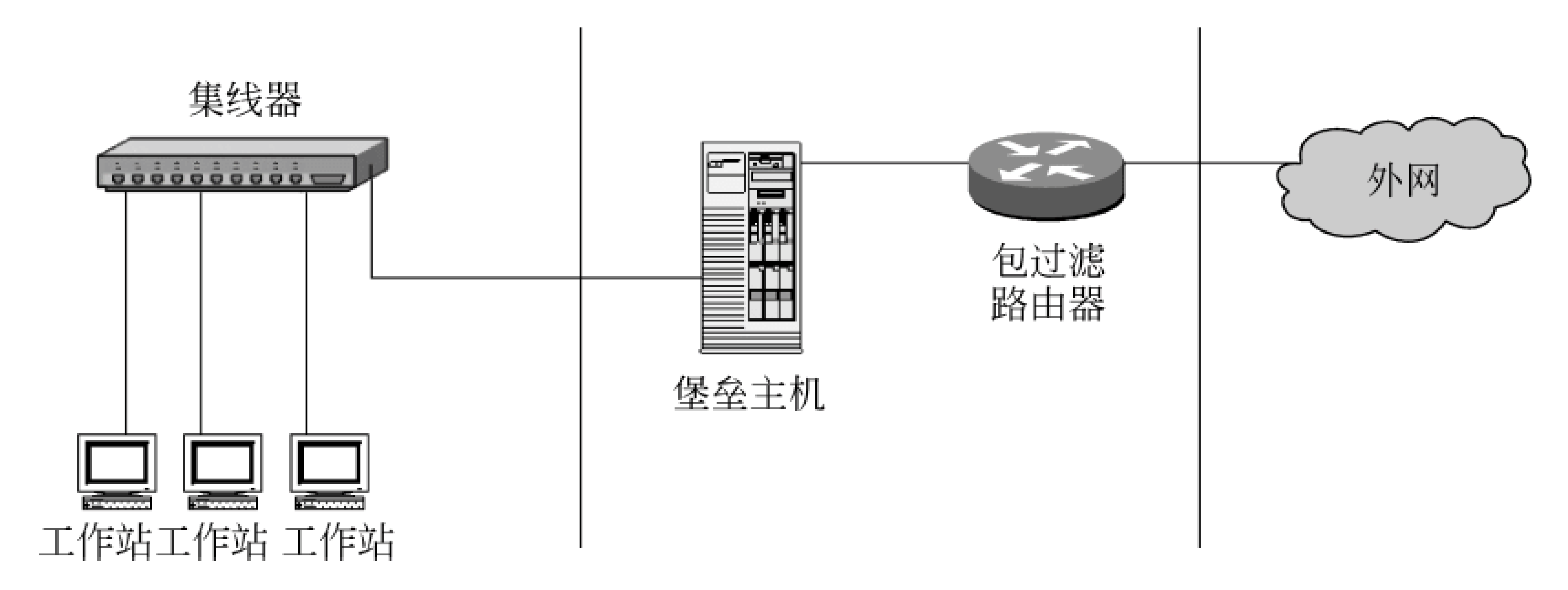


图 8-16　双宿堡垒主机

数据流，Intranet 和 Internet 均可访问屏蔽子网，但禁止它们穿过屏蔽子网通信。可根据需要在屏蔽子网中安装堡垒主机，为内部网络和外部网络的互相访问提供代理服务，但是来自两网络的访问都必须通过两个包过滤路由器的检查。

对于向 Internet 公开的服务器，像 WWW、FTP、Mail 等 Internet 服务器也可安装在屏蔽子网内，这样无论是外部用户，还是内部用户都可访问。屏蔽子网的防火墙安全性能高，具有很强的抗攻击能力，但需要的设备多，造价高。屏蔽子网如图 8-17 所示。

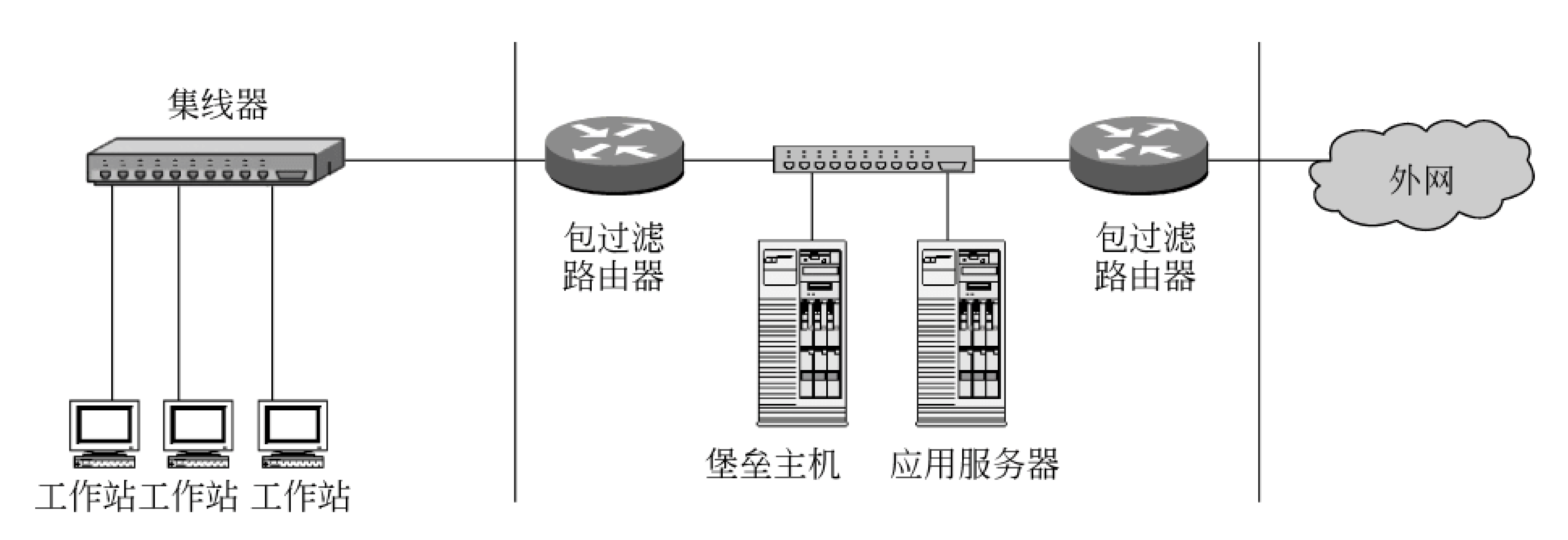


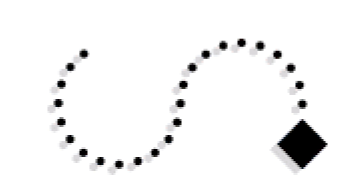
图 8-17　屏蔽子网

当然，防火墙本身也有其局限性，如不能防范绕过防火墙的入侵，一般的防火墙不能防止受到病毒感染的软件或文件的传输，难以避免来自内部的攻击等。总之，防火墙只是一种整体安全防范策略的一部分，仅有防火墙是不够的，安全策略还必须包括全面的安全准则，即网络访问、本地和远程用户认证、拨入拨出呼叫、磁盘和数据加密以及病毒防护等有关的安全策略。

8.3　计算机病毒

8.3.1　计算机病毒的特点及分类

计算机病毒是一种计算机程序，是一段可执行的指令代码。就像生物病毒一样，计算机病毒有独特的复制能力，可以很快地蔓延，又非常难根除。计算机病毒不是来源于突发或偶然的原因的。一次突发的停电和偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的。计算机病毒则是一种比较完美的、精巧严谨的代



码,按照严格的秩序组织起来,并与所在的系统网络环境配合起来对系统进行破坏。

多数病毒可以找到作者信息和产地信息,通过大量的资料分析统计来看,编写病毒的目的是:一些天才的程序员为了表现和证明自己的能力、出于对上司的不满、为了好奇、为了祝贺和求爱等,当然也有因政治、军事、宗教、民族、专利等方面的需求而专门编写的。

计算机病毒在《中华人民共和国计算机信息系统安全保护条例》中被明确定义为:"编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。"

1. 计算机病毒的特点

具有很强的传染性、一定的潜伏性、特定的触发性、很大的破坏性,如图 8-18 所示。

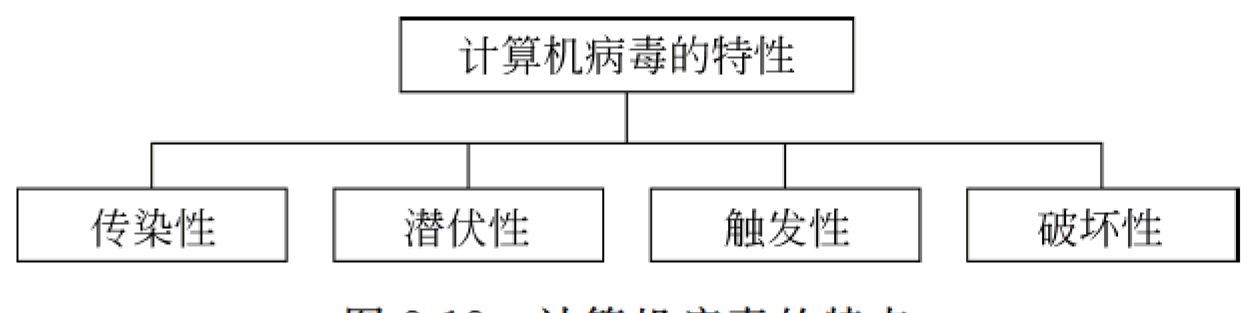


图 8-18　计算机病毒的特点

传染性是病毒的基本特征。在生物界,病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下,病毒可得到大量繁殖,使被感染的生物体表现出病症甚至死亡。同样,计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机,在某些情况下造成被感染的计算机工作失常甚至瘫痪。

与生物病毒不同的是,计算机病毒是一段人为编制的计算机程序代码,这段程序代码一旦进入计算机并得以执行,就会搜寻其他符合其传染条件的程序或存储介质,确定目标后再将自身代码插入其中,达到自我繁殖的目的。只要一台计算机染毒,如不及时处理,那么病毒就会在这台机子上迅速扩散,其中的大量文件(一般是可执行文件)会被感染。而被感染的文件又成了新的传染源,在与其他机器进行数据交换或通过网络接触时,病毒会继续进行传染。

正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的,而计算机病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道,如软盘、计算机网络去传染其他的计算机。如果在一台机器上发现了病毒,往往曾在这台计算机上用过的软盘也已感染上了病毒,而与这台机器相联的其他计算机可能也被该病毒传染上了。是否具有传染性是判别一个程序是否为计算机病毒最重要的条件。

潜伏性的第一种表现是指病毒程序不用专用检测程序是检查不出来的,因此病毒可以静静地躲在磁盘或磁带里待上几天,甚至几年,一旦时机成熟,病毒得到运行机会,就又四处繁殖、扩散,继续为害。

潜伏性的第二种表现是指计算机病毒的内部往往有一种触发机制,不满足触发条件时,计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足,有的在屏幕上显示信息、图形或特殊标识,有的则执行破坏系统的操作,如格式化磁盘、删除磁盘文件、对数据文件进行加密、封锁键盘以及使系统死机等。

病毒因某个事件或数值的出现,诱使病毒实施感染或进行攻击的特性称为可触发性。

为了隐蔽自己，病毒必须潜伏，少做动作。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，就启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，就使病毒继续潜伏。

计算机病毒的破坏性主要取决于计算机病毒设计者的目的，如果病毒设计者的目的在于彻底破坏系统的正常运行，那么这种病毒对于计算机系统进行攻击造成的后果将是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复，但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统崩溃等重大恶果。

2. 计算机病毒的分类

病毒从不同的角度有不同的分类。按危害性分为良性病毒和恶性病毒；按寄生方式分为代替式病毒、链接式病毒、转储式病毒、填充式病毒和覆盖式病毒等。按病毒感染的途径，病毒分为4类。

(1) 操作系统型病毒(Operating System Viruses)。这类病毒程序作为操作系统的一个模块在系统中运行，一旦激发，它就工作。例如，它作为操作系统的引导程序时，计算机一旦启动就首先运行病毒程序，然后才启动操作系统程序。这类病毒也称为引导型病毒，如小球病毒、大麻病毒等。

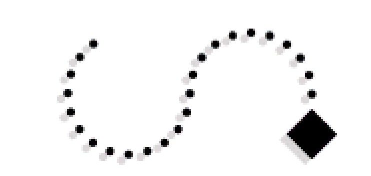
(2) 文件型病毒(File Viruses)。文件型病毒攻击的对象是文件，并寄生在文件中，当文件运行时，首先运行病毒程序，然后才运行指定的文件(这类文件一般是可执行文件)。文件型病毒又称为外壳型(Shell Viruses)型病毒，其病毒程序包围在宿主程序的外围，对其宿主程序不修改。

感染文件的病毒有Jerusalem、Yankee Doole、Liberty、1575、Traveller、4096等，主要感染.com和.exe文件。这类病毒增加了被感染的文件字节数，并且病毒代码主体没有加密，也容易被查出和解除。在文件型病毒中，略有对抗反病毒手段的只有Yankee Doole病毒，当它发现用Debug工具跟踪时，会自动从文件中逃走。

(3) 复合型病毒。复合型病毒既感染文件，又感染引导扇区，常见的有XqR(New century)、Invader(侵入者)、Plastique(塑料炸弹)、3584(郑州狼)、ALFA/3072-2、Ghost/One Halff3544(幽灵)等。如果只清除了文件或硬盘主引导扇区的病毒，则仍会感染系统。解决的方法是从软盘启动系统，然后调用软盘版杀毒软件，同时杀掉硬盘上的引导扇区病毒和文件病毒。

(4) 宏病毒。宏病毒主要是利用软件本身所提供的宏能力来设病毒的，所以凡是具有宏能力的软件都有宏病毒存在的可能，如Word、Excel。Microsoft Word中把宏定义为"能组织到一起作为独立的命令的一系列Word命令，它能使日常工作变得更容易。"而Word宏病毒利用Word的开放性，即Word中提供的WordBasic编程接口，并能通过doc文档及doc模板进行自我复制及传播。

随着Office新版本的推出，微软不断加强宏的功能，宏病毒的危害也越来越大。Melissa病毒是利用宏来使E-mail管理程序Outlook自动根据其通讯录中记录的前50个地址发信，而July Killer宏病毒的破坏方式则是产生一个只有一条指令deltree/y C:\的Autoexec.bat文件来替代现有的该文件，当下次启动计算机时，这条指令就会删除C盘中的



所有文件,所以宏病毒是一种危害极大的病毒。

8.3.2 计算机病毒的工作过程

1. 计算机病毒程序的结构

计算机病毒包括三大功能块,即引导模块、传播模块和破坏/表现模块。其中,后两个模块各包含一段触发条件检查代码,它们分别检查是否满足传染触发的条件和是否满足表现触发的条件,只有在相应的条件满足时,病毒才会进行传染或表现/破坏。必须指出,不是任何病毒都必须包括这三个模块的,有些病毒没有引导模块,有些病毒没有破坏模块。

三个模块各自的作用是:引导模块将病毒由外存引入内存,使后两个模块处于活动状态;传播模块用来将病毒传染到其他对象上去;破坏/表现模块实施病毒的破坏作用,如删除文件、格式化磁盘等,由于该模块中有些病毒并没有明显的恶意破坏作用,只是进行一些视屏或发声方面的自我表现作用,故该模块有时又称为表现模块。计算机病毒程序结构,如图 8-19 所示。



图 8-19 计算机病毒程序结构

2. 计算机病毒的引导及传染

目前的计算机病毒寄生对象有两种,一是寄生在磁盘的引导区上;二是寄生在可执行文件上。

对于寄生在磁盘引导区的病毒来说,病毒引导程序占用了原引导程序的位置,并将原引导程序转移到一个特定的地方。这样系统一启动,病毒就被引导进内存并获得执行权,然后将病毒的其他两个模块装入内存,采取常驻内存技术以保证这两个模块不会被覆盖,并设定激活方式,使之能在适当的方式下被激活。然后病毒引导程序将系统引导模块装入内存,使系统在带毒状态下工作。

对于寄生在可执行文件中的病毒来说,病毒程序通过修改原有的可执行文件,一般链接在可执行文件的首部、中间、尾部等,将病毒引导程序引入内存,该引导程序将病毒的其他两个模块装入内存,并完成驻留内存及初始化工作,然后将执行权交给执行文件,使系统在带病的状态下工作。

传染是指计算机病毒由一个载体传播到另一个载体或者由一个系统进入另一个系统的过程。用户在复制磁盘或文件时,把一个病毒由一个载体复制到另一个载体上。或者通过网络上的信息传递,把一个病毒程序从一方传递到另一方,这种传染方式叫做计算机病毒的被动传染。在病毒处于激活的状态下,只要传染条件满足,病毒程序就能主动地把病毒自身传染给另一个载体或另一个系统,这种传染方式叫做计算机病毒的主动传染。

对于病毒的被动传染而言,其传染过程是随着复制磁盘或文件工作的进行而进行的。而对于计算机病毒的主动传染而言,其传染过程是这样的:在系统运行时,病毒通过病毒载体即系统的外存储器进入系统的内存储器,常驻内存,并在系统内存中监视系统的运行。

在病毒引导模块将病毒传播模块驻留内存的过程中,通常还要修改系统中断向量入口地址(例如 INT 13H 或 INT 21H),使该中断向量指向病毒程序传播模块。这样一旦系统执行磁盘读写操作或系统功能调用,病毒传播模块就被激活,传播模块在判断传染条

件满足的条件下，利用系统INT 13H读写磁盘中断把病毒自身传播给被读写的磁盘或被加载的程序，也就是实施病毒的传染，然后再转移到原中断服务程序执行原有的操作。

3. 病毒的触发

进入内存处于运行状态的病毒，并不是马上就起破坏作用的，还要等待一定的触发条件。在触发条件的设置上要兼顾潜伏性与杀伤力，过于苛刻和宽泛都会影响计算机病毒的破坏性。计算机病毒采用的常见的触发条件有7种：

(1) 日期触发。许多病毒采用日期做触发条件。日期触发包括特定日期触发、月份触发、前半年后半年触发等。

(2) 时间触发。时间触发包括特定的时间触发、染毒后累计工作时间触发、文件最后写入时间触发等。

(3) 键盘触发。有些病毒监视用户的按键动作，出现病毒预定的输入时、病毒被激活，进行某些特定操作。键盘触发包括按键次数触发、组合键触发、热启动触发等。

(4) 感染触发。许多病毒的感染需要某些条件触发，而且相当数量的病毒又以与感染有关的信息反过来作为破坏行为的触发条件，称为感染触发。感染触发包括运行感染文件个数触发、感染次数触发、感染磁盘数触发、感染失败触发等。

(5) 启动触发。病毒对机器的启动次数计数，并将此值作为触发条件，称为启动触发。

(6) 访问磁盘次数触发。病毒对磁盘I/O访问的次数进行计数，以预定次数做触发条件，称为访问磁盘次数触发。

(7) 调用中断功能触发。病毒对中断调用次数计数，以预定次数作为触发条件。

4. 计算机病毒的工作过程

计算机病毒的工作过程，如图8-20所示。

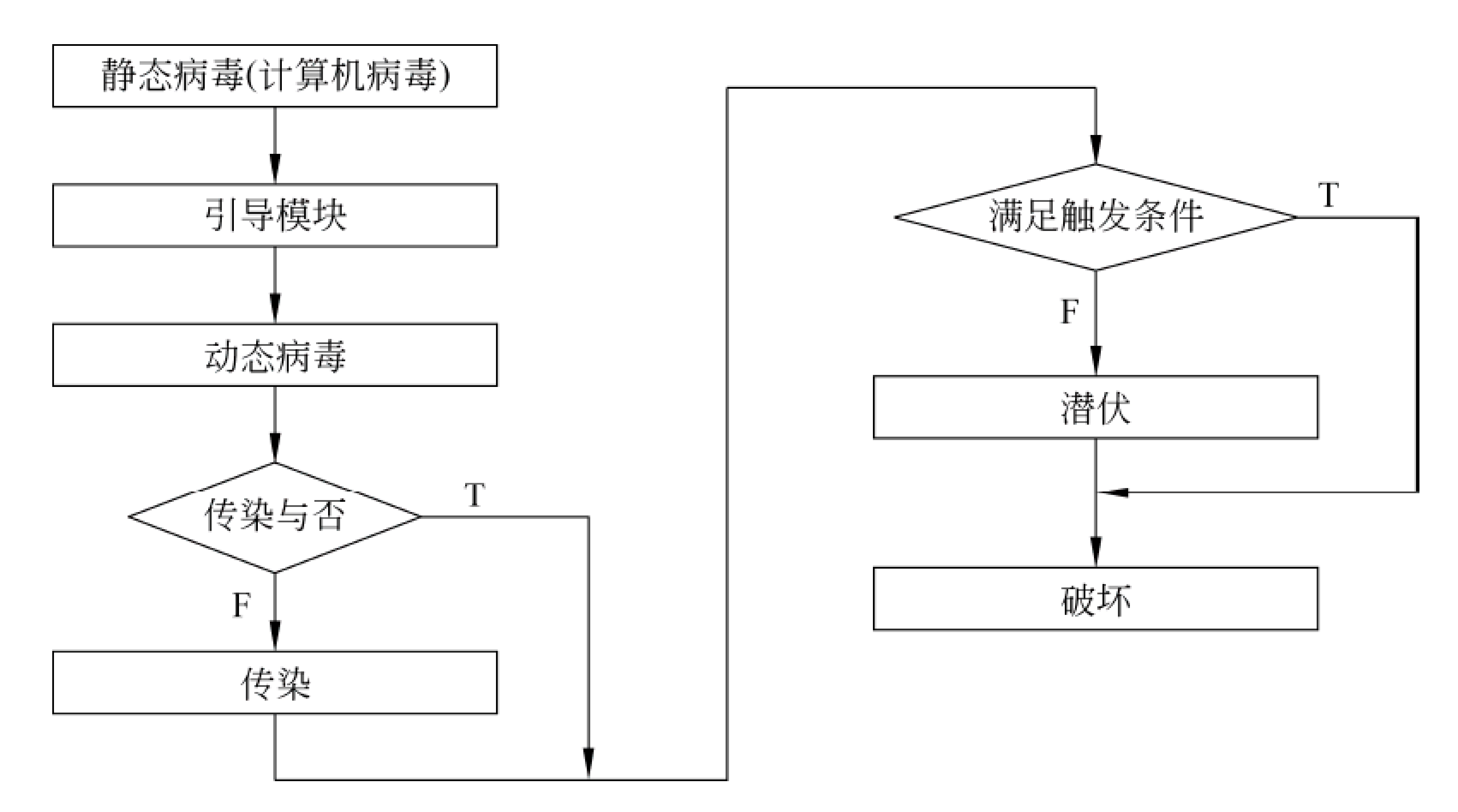
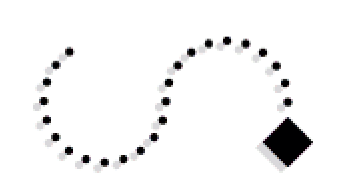


图8-20 计算机病毒的工作过程

8.3.3 计算机反病毒技术

计算机病毒学鼻祖早在20世纪80年代初期就提出了计算机病毒的模型，证明只要



延用现行的计算机体系，计算机病毒就存在不可判定性。杀病毒必须先搜集到病毒样本，使其成为已知病毒，然后剖析病毒，再将病毒传染的过程准确地颠倒过来，使被感染的计算机恢复原状。因此可以看出，一方面计算机病毒是不可灭绝的，另一方面病毒也并不可怕，世界上没有杀不掉的病毒。

1. 反病毒技术分类

从研究的角度，反病毒技术主要分以下三类。

(1) 预防病毒技术。预防病毒技术自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏，主要手段包括加密可执行程序、引导区保护、系统监控与读写控制等。

(2) 检测病毒技术。通过对计算机病毒的特征来进行判断的侦测技术，如自身校验、关键字等。

(3) 消除病毒技术。通过对病毒的分析，杀除病毒并恢复原文件。

2. 反病毒实现技术

从具体实现技术的角度，常用的反病毒技术有以下 6 种。

(1) 病毒代码扫描法。将新发现的病毒加以分析后根据其特征编成病毒代码，加入病毒特征库中。每当执行杀毒程序时，便立刻扫描程序文件，并与病毒代码比对，便能检测到是否有病毒。病毒代码扫描法速度快、效率高。使用特征码技术需要实现一些补充功能，例如近来的压缩包、压缩可执行文件自动查杀技术。大多数防毒软件均采用这种方式，但是无法检测到未知的新病毒以及变种病毒。

(2) 人工智能陷阱(Rule-based)。它是一种监测计算机行为的常驻式扫描技术。它将所有病毒所产生的行为归纳起来，一旦发现内存的程序有任何不当的行为，系统就会有所警觉，并告知用户。其优点是执行速度快，手续简便，且可以检测到各种病毒；其缺点是程序设计难，且不容易考虑周全。

(3) 软件模拟扫描法。它专门用来对付千面人病毒(Polymorphic/Mutation Virus)。千面人病毒在每次传染时，都以不同的随机数加密于每个中毒的文件中，传统病毒代码比对的方式根本就无法找到这种病毒。软件模拟技术则成功地模拟 CPU 执行，在其设计的 DOS 虚拟机器(Virtual Machine)下模拟执行病毒的变体引擎解码程序，将多形体病毒解开，使其显露原来的面目，再加以扫描。目前虚拟机的处理对象主要是文件型病毒。

对于引导型病毒、Word/Excel 宏病毒、木马程序在理论上都是可以通过虚拟机来处理的，但目前的实现水平仍相距甚远。就像病毒编码变形使得传统特征值方法失效一样，针对虚拟机的新病毒可以轻易地使得虚拟机失效。虽然虚拟机也会在实践中不断发展。但是，PC 的计算能力有限，反病毒软件的制造成本也有限，而病毒的发展可以说是无限的。让虚拟技术获得更加实际的功效，甚至要以此为基础来清除未知病毒，其难度相当大。

(4) 先知扫描法 VICE(Virus Instruction Code Emulation)。它是继软件模拟技术后的一大突破。既然软件模拟可以建立一个保护模式下的 DOS 虚拟机器，模拟 CPU 动作并模拟执行程序以解开变体引擎病毒，那么类似的技术也可以用来分析一般程序检查可疑的病毒代码。因此，VICE 将工程师用来判断程序是否有病毒代码存在的方法，分析归

纳成专家系统知识库，再利用软件工程的模拟技术（Software Emulation）执行新的病毒，就可分析出新病毒代码对付以后的病毒。

该技术是专门针对于未知的计算机病毒所设计的，利用这种技术可以直接模拟CPU的动作来侦测出某些变种病毒的活动情况，并且研制出该病毒的病毒码。由于该技术较其他解毒技术严谨，对于比较复杂的程序在病毒代码比对上会耗费比较多的时间，所以该技术的应用不那么广泛。

（5）文件宏病毒陷阱（Macro Trap TM）。它结合了病毒代码比对与人工智慧陷阱技术，根据病毒行为模式（Rule base）来检测已知及未知的宏病毒。其中，配合对象链接与嵌套（Object Linking and Embedding）技术，可将宏与文件分开，回快扫描，并可有效地将宏病毒彻底清除。

（6）主动内核技术（Active Kernel）。它将已经开发的各种网络防病毒技术从源程序级嵌入操作系统或网络系统的内核中，实现网络防病毒产品与操作系统的无缝连接。这种技术可以保证网络防病毒模块从系统的底层内核与各种操作系统和应用环境密切协调，确保防毒操作不会伤及操作系统内核，同时确保杀灭病毒的功效。

8.3.4 计算机病毒举例

1. CIH病毒

CIH病毒属于文件型病毒，只感染Windows 9x操作系统下的可执行文件。当受感染的.exe文件执行后，该病毒便驻留内存中，并感染所接触到的其他PE（Portable Executable）格式执行程序。

随着技术更新的频率越来越快，主板生产厂商使用EPROM来做BIOS的存储器，这是一种可擦写的ROM。通常所说的BIOS升级就是借助特殊程序修改ROM中BIOS里的固化程序。采用这种可擦写的EPROM，虽然方便了用户及时对BIOS进行升级处理，但同时也给病毒带来了可乘之机。CIH的破坏性在于它会攻击BIOS、覆盖硬盘、进入Windows内核。

（1）攻击BIOS。当CIH发作时，它会试图向BIOS写入垃圾信息，BIOS中的内容会被彻底洗去。

（2）覆盖硬盘。CIH发作时，调节器用IOS-Send Command直接对硬盘进行存取，将垃圾代码以208个扇区为单位，循环写入硬盘，直到所有硬盘上的数据均被破坏为止。

（3）进入Windows内核。无论是要攻击BIOS，还是设法驻留内存来为病毒传播创造条件，对CIH这类病毒而言，关键是要进入Windows内核，取得核心级控制权。

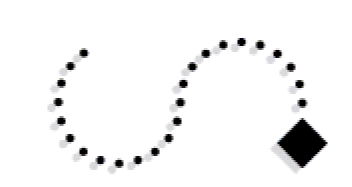
为防范CIH病毒对计算机主板的破坏，需采取一些针对性的措施。

（1）修改系统时间，跳过病毒的发作日。

（2）有些计算机系统主板具备BIOS写保护跳线，但一般设置均为开，可将其拨至关的位置，这样可以防止病毒向BIOS写入信息。

（3）检查CIH病毒可采用压缩并解压缩文件的方式，如果解压缩出现问题，多半可以肯定有CIHV1.2病毒的存在，但用该方法不能判断CIHV1.4病毒。

（4）用户不要轻易启动从电子邮件或从网站上下载的未知软件。



（5）由于病毒将垃圾码写入硬盘，导致硬盘的数据不能恢复，务必将重要数据备份，以免造成损失。

2. 蠕虫病毒

蠕虫病毒的编写相对其他形式的病毒程序来说简单一些，它可以用 VB 语言、C 语言或者传统语言来编写，还可以 wsh 脚本宿主，如常见的 VBScript 和 JavaScript 等语言来编写。但这并不意味着这种程序的破坏性小，相反，它具有极强的破坏能力，并且由于有 Internet 这个传播的大好场所，它有着将传统病毒挤出市场的趋势。

蠕虫病毒与一般的计算机病毒不同，它不采用将自身复制并附加到其他程序中，所以在病毒中也算是一个“另类”。脚本病毒也是很容易制造的，都利用了 Windows 系统的开放性，特别是 com 到 com＋的组件编程思路，一个脚本程序调用功能更大的组件来完成自己的功能。它们相对来说较其他的病毒容易编写。

蠕虫病毒与普通病毒的区别如表 8-4 所示。

表 8-4　蠕虫病毒与普通病毒的区别

病毒分类 / 病毒属性	普 通 病 毒	蠕 虫 病 毒
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

8.4　黑客的攻击技术简介

黑客是英文 hacker 的音译，hacker 这个单词源于动词 hack，原是指热心于计算机技术且水平高超的计算机专家，尤其是程序设计人员。他们非常精通计算机硬件和软件知识，对操作系统和程序设计语言有着全面深刻的认识，善于探索计算机系统的奥秘，发现系统中的漏洞及原因所在。他们信守永不破坏任何系统的原则，检查系统的完整性和安全性，并乐于与他人共享研究成果。

到今天，黑客一词已被用于泛指那些未经许可就闯入计算机系统进行破坏的人。他们中的一些人利用漏洞进入计算机系统后，破坏重要的数据。另一些人利用黑客技术控制别人的计算机，从中盗取重要资源、干起非法勾当，他们已经成了入侵者和破坏者。

造成网络不安全的主要因素有系统、协议及数据库等设计上存在的缺陷。由于当今的计算机网络操作系统在本身结构设计和代码设计时偏重考虑系统使用时的方便性，导致系统在远程访问、权限控制和口令管理等许多方面存在安全漏洞。网络互联一般采用 TCP/IP，它是一个工业标准的协议簇，但该协议簇在制订之初，对安全问题考虑不多，协议中有很多的安全漏洞。同样，数据库管理系统（DBMS）也存在数据的安全性、权限管理及远程访问等方面的问题。例如，在 DBMS 或应用程序中可以预先安装从事情报收集、受控激发、定时发作等破坏程序。

8.4.1 黑客的进攻过程

黑客的进攻过程如图 8-21 所示。

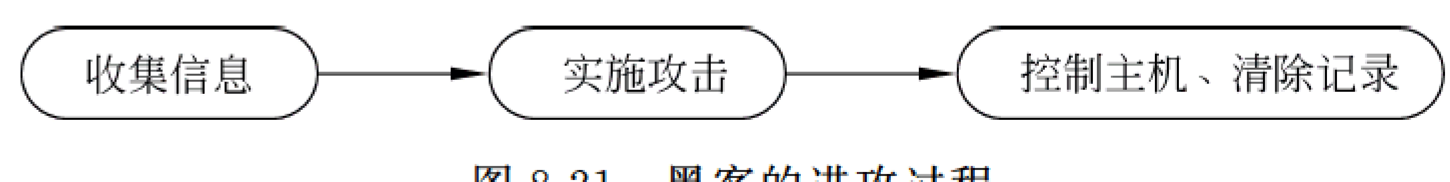


图 8-21 黑客的进攻过程

1. 收集信息

黑客在发动攻击前需要锁定目标，了解目标的网络结构，收集各种目标系统的信息。

(1) 锁定目标。网络上有许多主机，黑客首先要寻找目标站点。能真正标识主机的是 IP 地址，黑客利用域名和 IP 地址就可以顺利地找到目标主机。

(2)了解目标的网络结构。确定要攻击的目标后，黑客就会设法了解其所在的网络结构，哪里是网关、路由，哪里有防火墙，哪些主机与要攻击的目标主机关系密切等，最简单地就是用 tracert 命令追踪路由，也可以发一些数据包看其是否能通过，猜测其防火墙过滤规则的设定等。当然老练的黑客在干这些的时候都会利用别的计算机来间接地探测，从而隐藏他们真实的 IP 地址。

(3) 收集系统信息。在收集到目标的网络信息之后，黑客会对网络上的每台主机进行全面的系统分析，以寻求该主机的安全漏洞或安全弱点。收集系统信息的方法有：开放端口分析、利用信息服务。

首先黑客要知道目标主机采用的是什么操作系统的什么版本，如果目标主机开放 Telnet 服务，黑客只要 Telnet 目标主机，就会显示系统的登录提示信息；接着黑客还会检查其开放端口进行服务分析，看是否有能被利用的服务。

WWW、Mail、FTP、Telnet 等日常网络服务，通常情况下 Telnet 服务的端口是 23，WWW 服务的端口是 80，FTP 服务的端口是 23。利用信息服务，像 SNMP 服务、Traceroute 程序、Whois 服务可以用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。Traceroute 程序能够获得到达目标主机所要经过的网络数和路由器数。Whois 协议服务能提供所有有关的 DNS 域和相关的管理参数。

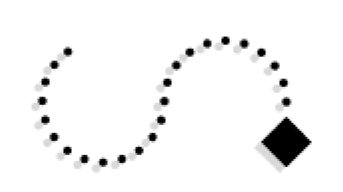
Finger 协议可以用 Finger 服务来获取一个指定主机上的所有用户的详细信息(如用户注册名、电话号码、最后注册时间以及他们有没有读邮件等)，所以如果没有特殊的需要，管理员就应该关闭这些服务。收集系统信息当然少不了利用扫描器来帮他们发现系统的各种漏洞，包括各种系统服务漏洞，应用软件漏洞，CGI ，弱口令用户等。

2. 实施攻击

当黑客探测到了足够的系统信息，对系统的安全弱点有了了解后就会发动攻击，当然他们会根据不同的网络结构、不同的系统情况而采用不同的攻击手段。一般黑客攻击的终极目的是能够控制目标系统，窃取其中的机密文件等，但并不是每次黑客攻击都能够达到控制目标主机的目的的，所以有时黑客也会发动拒绝服务攻击之类的干扰攻击，使系统不能正常工作。

3. 控制主机并清除记录

黑客利用种种手段进入目标主机系统并获得控制权之后，不会马上进行破坏活动，删



除数据、涂改网页等。一般入侵成功后,黑客为了能长时间地保留和巩固他对系统的控制权,不被管理员发现,他会做两件事:清除记录和留下后门。日志往往会记录一些黑客攻击的蛛丝马迹,黑客当然不会留下这些"犯罪证据",他会删除日志或用假日志覆盖它。为了日后可以不被觉察地再次进入系统,黑客会更改某些系统设置、在系统中置入特洛伊木马或其他一些远程操作程序。也可能什么都不动,只是把目标主机的系统作为他存放黑客程序或资料的仓库,黑客也可能会利用这台已经攻陷的主机去继续他下一步的攻击,如继续入侵内部网络,或者利用这台主机发动DOS攻击使网络瘫痪。

8.4.2 黑客常用的攻击方法

计算机系统中存在的安全隐患,便成为黑客进行攻击的地方,黑客创造了多种攻击方法,常用的攻击方法如图8-22所示。

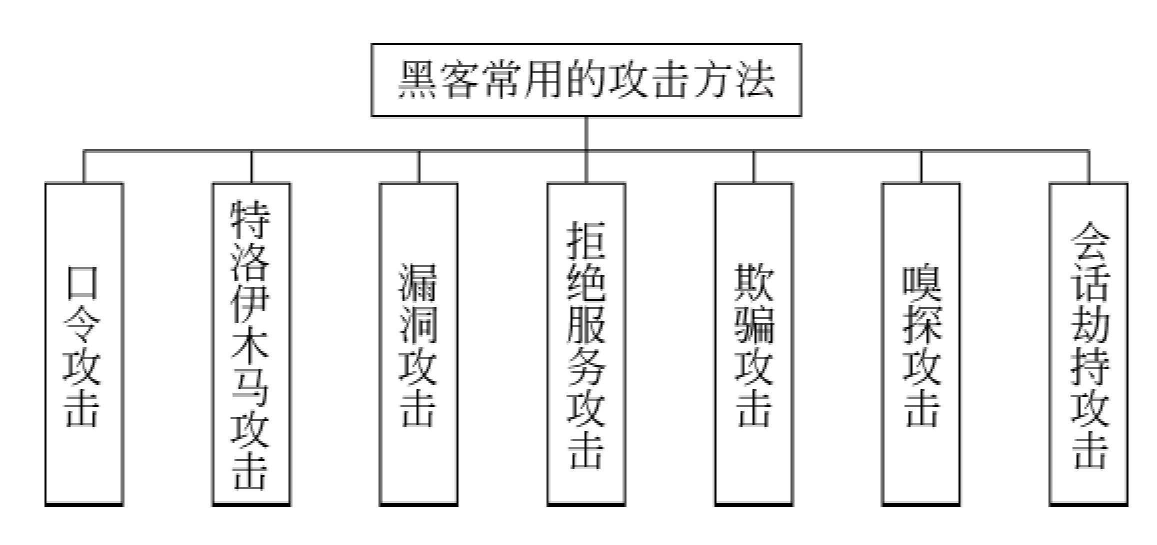


图8-22 黑客常用的攻击方法

1. 口令攻击

口令攻击是黑客最老牌的攻击方法,从黑客诞生的那天起它就开始被使用,这种攻击方式有三种:

(1) 暴力破解法。在知道用户的账号后用一些专门的软件强行破解用户口令(包括远程登录破解和对密码存储文件Passwd、Sam的破解)。这种方法要有足够的耐心和时间,但总有那么一些使用简单口令的用户账号,使得黑客可以迅速将其破解。

(2) 伪造登录界面法。在被攻击主机上启动一个可执行程序,该程序显示一个伪造的登录界面,当用户在这个伪装的界面上输入用户名、密码后,程序就将用户输入的信息传送到攻击者主机。

(3) 通过网络监听来得到用户口令。这种方法危害性很大,监听者往往能够获得其中一个网段的所有用户账号和口令。

2. 特洛伊木马攻击

特洛伊木马程序攻击也是黑客常用的攻击手段,黑客会编写一些看似"合法"的程序,但实际上此程序隐藏着其他非法功能,例如一个外表看似是一个有趣的小游戏的程序,实际运行的同时它在后台为黑客创建了一条访问你的系统的通道,这就是特洛伊木马程序。

当然只有当用户运行了木马后才会达到攻击的效果,所以黑客会把它上传到一些站点引诱用户下载,或者用E-mail寄给用户并编造各种理由骗用户运行它,当用户运行此软件后,该软件会悄悄执行它的非法功能:跟踪用户的计算机操作,记录用户输入的口令、上网账号等敏感信息,并把它们发送到黑客指定的电子信箱。如果是像冰河、灰鸽子

这样功能强大的远程控制木马，黑客还可以像在本地操作一样地远程操控用户的计算机。

3. 漏洞攻击

利用漏洞攻击是黑客攻击中最容易得逞的方法。许多系统及网络应用软件都存在着各种各样的安全漏洞，如 Windows 98 的共享目录密码验证漏洞，Windows 2000 的 Unicode、Printer、Ida、Idq、Webdav 漏洞，UNIX 的 Telnet、RPC 漏洞、Sendmail 的邮件服务软件漏洞，还有基于 Web 服务的各种 CGI 漏洞等，这些都是最容易被黑客利用的系统漏洞。特别是其中的一些缓冲区溢出漏洞，利用这些缓冲区溢出漏洞，黑客不但可以通过发送特殊的数据包来使服务或系统瘫痪，甚至可以精确地控制溢出后在堆栈中写入的代码，以使其能执行黑客的任意命令，从而进入并控制系统。

4. 拒绝服务攻击

拒绝服务攻击(DoS)是一种最悠久也是最常见的攻击形式，它利用 TCP/IP 的缺陷，将提供服务的网络资源耗尽，导致网络不能提供正常服务，是一种对网络危害巨大的恶意攻击。其实严格来说拒绝服务攻击并不是某一种具体的攻击方式，而是攻击所表现出来的结果，最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或崩溃。DoS 攻击方法可以是单一的手段，也可以是多种方式的组合利用，不过其结果都是一样的，即合法的用户无法访问所需的信息。

通常拒绝服务攻击可分为两种类型：一种攻击是黑客利用网络协议缺陷或系统漏洞发送一些非法的数据或数据包，使得系统死机或重新启动，从而使一个系统或网络瘫痪，如 Land 攻击、WinNuke、Ping of Death、TearDrop 等；另一种攻击是黑客在短时间内发送大量伪造的连接请求报文到网络服务所在的端口，例如 80 端口，从而消耗系统的带宽或设备的 CPU 和内存，造成服务器的资源耗尽，系统停止响应甚至崩溃，其中，具有代表性的攻击手段包括 SYN flood、ICMP flood、UDP flood 等。

分布式拒绝服务(DDoS)攻击是目前网络的头号威胁，是在传统的 DoS 攻击基础之上产生的一种攻击方式。单一的 DoS 攻击一般采用一对一攻击，而分布式的拒绝服务攻击是黑客控制多台计算机(可以是几台也可以是成千上万台)同时攻击，这样的攻击即使是一些大网站也很难抵御。

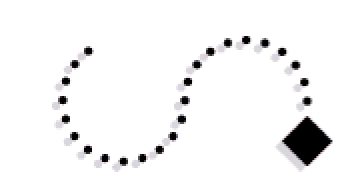
5. 欺骗攻击

常见黑客欺骗攻击方法有：IP 欺骗攻击、DNS 欺骗邮件欺骗攻击、网页欺骗攻击等。

(1) IP 欺骗攻击。黑客改变自己的 IP 地址，伪装成别人计算机的 IP 地址来获得信息或者得到特权。如 UNIX 机器之间能建立信任关系，使得这些主机的访问变得容易，而这个信任关系基本上是使用 IP 地址进行验证的，这样你就知道 IP 欺骗能干什么了吧。

(2) 电子信件欺骗攻击。黑客向某位用户发了一封电子邮件，并且修改了邮件头信息(使得邮件地址看上去和这个系统管理员的邮件地址完全相同)，信中他冒称自己是系统管理员，说由于系统服务器故障导致部分用户数据丢失，要求该用户把他的个人信息马上用 E-mail 回复给他，这就是一个典型的电子邮件欺骗攻击的例子。

(3) 网页欺骗攻击。黑客将某个站点的网页都复制下来，然后修改其链接，使得用户访问这些链接时先经过黑客控制的主机，然后黑客会想方设法让用户访问这个修改后的网页，他则监控用户的整个 HTTP 请求过程，窃取用户的账号和口令等信息，甚至假冒用



户给服务器发接数据。如果这个网页是电子商务站点，那用户的损失就可想而知了。

6. 嗅探攻击

要了解嗅探攻击方法，先要知道它的原理。网络的一个特点就是数据总是在流动中的，当数据从网络的一台计算机到另一台计算机的时候，通常会经过大量不同的网络设备，在传输过程中，有人可能会通过特殊的设备（嗅探器，有硬件和软件两种）捕获这些传输网络数据的报文。

嗅探攻击主要有两种途径，一种是针对简单的采用集线器（Hub）连接的局域网，黑客只要能把嗅探器安装到这个网络中的任何一台计算机上就可以实现对整个局域网的侦听，这是因为共享 Hub 获得一个子网内需要接收的数据时，并不是直接发送到指定主机，而是通过广播方式发送到每台计算机的。正常情况下，数据接受的目标计算机会处理该数据，而其他非接受者的计算机会过滤这些数据，但安装了嗅探器的计算机则会接收所有数据。

另一种是针对交换网络的，由于交换网络的数据是从一台计算机发送到预定的计算机，而不是广播的，所以黑客必须将嗅探器放到像网关服务器、路由器这样的设备上才能监听到网络上的数据，当然这比较困难，但一旦成功就能够获得整个网段的所有用户账号和口令，所以黑客还是会通过其他种种攻击手段来实现它的，如通过木马方式将嗅探器发给某个网络管理员，使其不自觉地为攻击者进行了安装。

7. 会话劫持攻击

假设某黑客在暗地里等待着某位合法用户通过 Telnet 远程登录到一台服务器上，当这位用户成功地提交密码后，这个黑客就开始接管该用户当前的会话并摇身变成这个用户，这就是会话劫持攻击。在一次正常的通信过程中，黑客作为第三方参与其中，或者是在数据流（例如基于 TCP 的会话）里注射额外的信息，或者是将双方的通信模式暗中改变，即从直接联系变成有黑客联系。会话劫持是一种结合了嗅探以及欺骗技术在内的攻击手段，最常见的是 TCP 会话劫持，像 HTTP、FTP、Telnet 都可能被进行会话劫持。

要实现会话劫持，黑客首先必须窥探到正在进行 TCP 通信的两台主机之间传送的报文源 IP、源 TCP 端口号、目的 IP、目的 TCP 端号，从而推算出其中一台主机将要收到的下一个 TCP 报文段中的 seq 和 ackseq 值，这样在该合法主机收到另一台合法主机发送的 TCP 报文前，攻击者根据所截获的信息向该主机发出一个带有净荷的 TCP 报文，如果该主机先收到攻击报文，就可以把合法的 TCP 会话建立在攻击主机与被攻击主机之间。带有净荷的攻击报文能够使被攻击主机对下一个要收到的 TCP 报文中的确认序号（ackseq）的值的要求发生变化，从而使另一台合法的主机向被攻击主机发出的报文被拒绝。

会话劫持攻击避开了被攻击主机对访问者的身份验证和安全认证，从而使黑客能直接进入被攻击主机，对系统安全构成的威胁比较严重。实现会话劫持攻击不但需要复杂的技术，而且还需要对攻击时间的精确把握，所以会话劫持攻击并不是太常见。

8.4.3　黑客的常用工具

黑客工具是指编写出来的用于网络安全方面的工具软件，其功能是支持网络攻击过程。下面对黑客的工具进行简单的介绍。

1. 扫描类软件

扫描是黑客的眼睛，通过扫描程序，黑客可以找到攻击目标的 IP 地址、开放的端口号、服务器运行的版本、程序中可能存在的漏洞等。根据不同的扫描目的，扫描类软件又分为地址扫描器、端口扫描器、漏洞扫描器三个类别。

在很多人看来，这些扫描器获得的信息大多数都是没有用处的，然而在黑客看来，扫描器好比黑客的眼睛，它可以让黑客清楚地了解目标，有经验的黑客则可以将目标“摸得一清二楚”，这对于攻击来说是至关重要的。同时扫描器也是网络管理员的得力助手，网络管理员可以通过扫描器了解自己系统的运行状态和可能存在的漏洞，在黑客“下手”之前将系统中的隐患清除，保证服务器的安全稳定。扫描器类软件有流光、SuperScan、X-way 等。SuperScan 的界面如图 8-23 所示。



图 8-23　SuperScan 的界面

2. 远程监控类软件

远程监控也叫做“木马”，这种程序实际上是在服务器上运行一个客户端软件，同时在黑客的计算机中运行一个服务端软件，如此一来，服务器将会变成黑客的服务器的“手下”，也就是说黑客将会利用木马程序在服务器上开一个端口，通过这种特殊的木马功能对服务器进行监视、控制。因此，只要黑客掌握了某个木马的使用和操作方法，就可以轻易接管网络服务器或者其他上网者的计算机。

在控制了服务器之后，黑客的攻击行动也就接近尾声了，然而在攻击之前，黑客必须想办法让服务器运行木马的客户端程序，这就需要利用漏洞或者进行欺骗。远程监控类软件有冰河、灰鸽子等。冰河软件的界面如图 8-24 所示。

3. 系统攻击和密码破解类软件

这类软件大多数都是由高级黑客编写出来供初级黑客使用的现成软件，软件本身不需要使用者具备太多知识，使用者只要按照软件说明操作就可以达到软件的预期目的。

系统攻击类软件主要分为信息炸弹和破坏炸弹。网络上常见的垃圾电子邮件就是这种软件的“杰作”，还有聊天室中经常看到的“踢人”、“骂人”类软件、论坛的垃圾灌水器、系统蓝屏炸弹也都属于此类软件的变异形式。

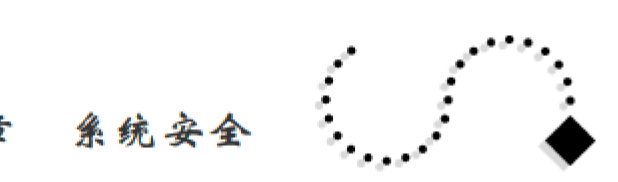




图 8-24 冰河软件界面

密码破解类软件可以帮助黑客寻找系统登录密码，相对于利用漏洞，暴力破解密码要简单许多，效率非常低，但是黑客无论是使用密码破解软件还是利用漏洞进入系统，都能达到入侵的目的。

常用的系统供给和密码破解类软件有溯雪、黑雨、网络刺客Ⅱ等。网络刺客Ⅱ软件的界面如图 8-25 所示。



图 8-25 网络刺客Ⅱ界面

4. 监听类软件

通过监听，黑客可以截获网络的信息包，之后对加密的信息包进行破解，进而分析包内的数据，获得有关系统的信息；也可能截获个人上网的信息包，获得用户的上网账号、系统账号、电子邮件账号等个人隐私资料。监听类软件有 Sinffit、nc、Capture Net 等。

CaptureNet 软件的界面如图 8-26 所示。

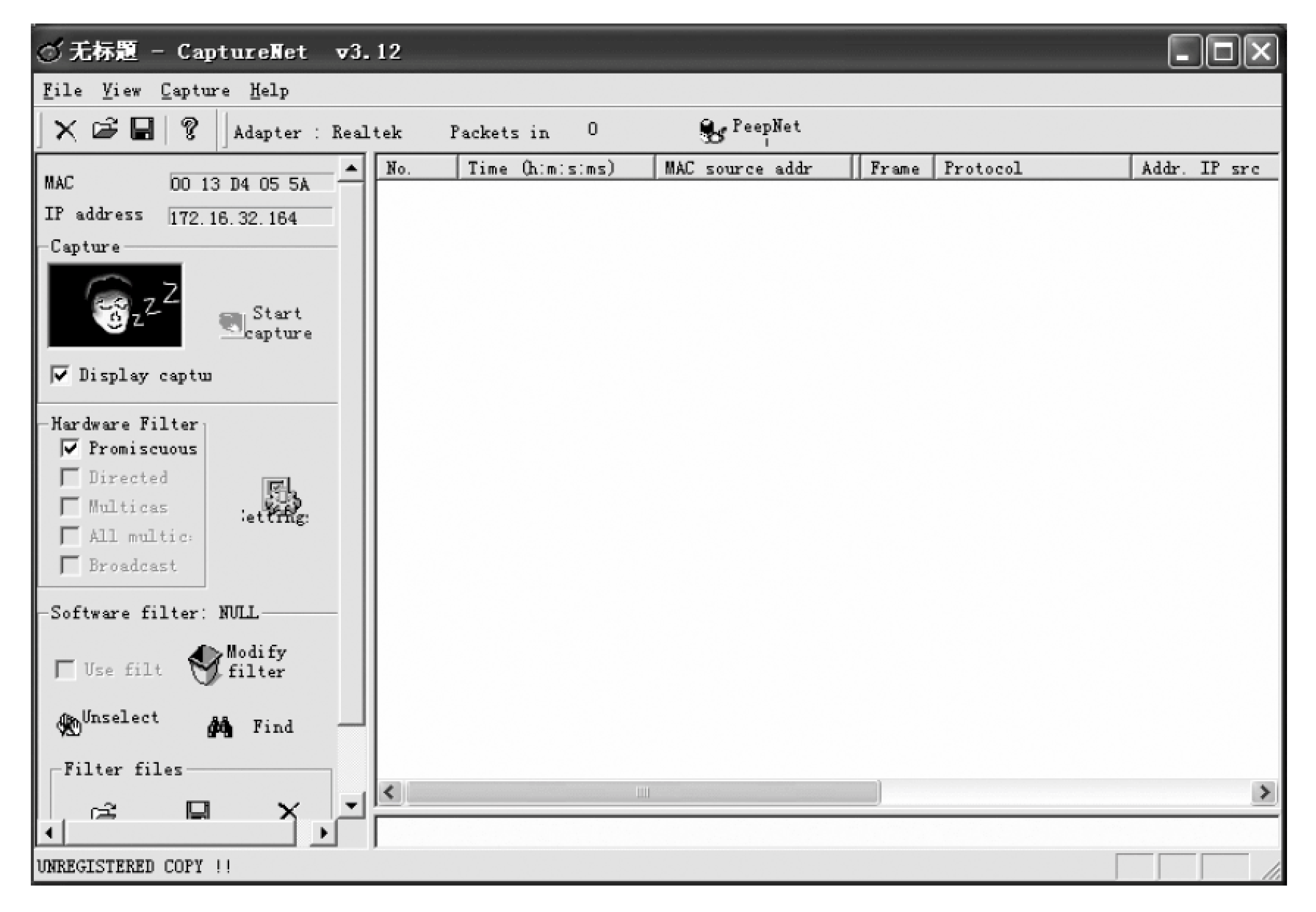


图 8-26 CaptureNet 界面

本章小结

本章主要介绍了加强计算机网络系统安全性的主要方法和技术手段。

在增强操作系统安全性上主要学习了 Windows 域模式下提高系统安全性的主要技术手段：身份认证和访问控制。这些工作都是操作系统在后台自动进行的，是网络环境下进行资源共享、信息共享的基础，对于它的学习有助于我们理解与之相关的网络设置和网络编程。

在增强系统安全性上，主要介绍了计算机病毒的特点、工作原理及常用的防病毒技术。同时还介绍了防火墙技术以及常用的防火墙的体系结构，通过学习了解到防火墙是进行内网、外网分隔的有效工具，同时体会到防病毒软件与防火墙在提高计算机网络安全性上的不同功用。最后简单介绍了破坏计算机网络系统的人——黑客，以及黑客常用的进攻手段和进攻过程。

本章习题

1. 简述 Windows 2003 进行身份认证的基本过程。
2. 简述计算机病毒的基本工作过程及主要的反病毒技术。
3. 简述防火墙的工作原理及体系结构。
4. 简述 CIH 病毒与蠕虫病毒的区别。

附录

信息安全等级保护管理办法

第一章　总　　则

第一条　为规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，制定本办法。

第二条　国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

第三条　公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

第四条　信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条　信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。

第二章　等级划分与保护

第六条　国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

第七条　信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级,信息系统受到破坏后,会对社会秩序和公共利益造成严重损害,或者对国家安全造成损害。

第四级,信息系统受到破坏后,会对社会秩序和公共利益造成特别严重的损害,或者对国家安全造成严重损害。

第五级,信息系统受到破坏后,会对国家安全造成特别严重的损害。

第八条 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护,国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

第三章 等级保护的实施与管理

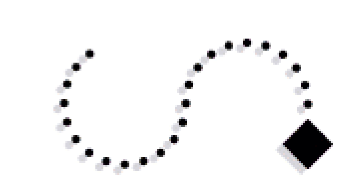
第九条 信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。

第十条 信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的,应当经主管部门审核批准。跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。对拟确定为第四级以上信息系统的,运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。

第十一条 信息系统的安全保护等级确定后,运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准,使用符合国家有关规定,满足信息系统安全保护等级需求的信息技术产品,开展信息系统安全建设或者改建工作。

第十二条 在信息系统建设过程中,运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》(GB 17859—1999)、《信息系统安全等级保护基本要求》等技术标准,参照《信息安全技术信息系统通用安全技术要求》(GB/T 20271—2006)、《信息安全技术网络基础安全技术要求》(GB/T 20270—2006)、《信息安全技术操作系统安全技术要求》(GB/T 20272—2006)、《信息安全技术数据库管理系统安全技术要求》(GB/T 20273—2006)、《信息安全技术服务器技术要求》、《信息安全技术终端计算机系统安全等级技术要求》(GA/T 671—2006)等技术标准同步建设符合该等级要求的信息安全设施。

第十三条 运营、使用单位应当参照《信息安全技术信息系统安全管理要求》(GB/T



20269—2006)、《信息安全技术信息系统安全工程管理要求》(GB/T 20282—2006)、《信息系统安全等级保护基本要求》等管理规范,制定并落实符合本系统安全保护等级要求的安全管理制度。

第十四条　信息系统建设完成后,运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构,依据《信息系统安全等级保护测评要求》等技术标准,定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评,第四级信息系统应当每半年至少进行一次等级测评,第五级信息系统应当依据特殊安全需求进行等级测评。信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查,第四级信息系统应当每半年至少进行一次自查,第五级信息系统应当依据特殊安全需求进行自查。经测评或者自查,信息系统安全状况未达到安全保护等级要求的,运营、使用单位应当制定方案进行整改。

第十五条　已运营(运行)的第二级以上信息系统,应当在安全保护等级确定后30日内,由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。新建第二级以上信息系统,应当在投入运行后30日内,由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。隶属于中央的在京单位,其跨省或者全国统一联网运行并由主管部门统一定级的信息系统,由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统,应当向当地设区的市级以上公安机关备案。

第十六条　办理信息系统安全保护等级备案手续时,应当填写《信息系统安全等级保护备案表》,第三级以上信息系统应当同时提供以下材料:

(一)系统拓扑结构及说明;

(二)系统安全组织机构和管理制度;

(三)系统安全保护设施设计实施方案或者改建实施方案;

(四)系统使用的信息安全产品清单及其认证、销售许可证明;

(五)测评后符合系统安全保护等级的技术检测评估报告;

(六)信息系统安全保护等级专家评审意见;

(七)主管部门审核批准信息系统安全保护等级的意见。

第十七条　信息系统备案后,公安机关应当对信息系统的备案情况进行审核,对符合等级保护要求的,应当在收到备案材料之日起的10个工作日内颁发信息系统安全等级保护备案证明;发现不符合本办法及有关标准的,应当在收到备案材料之日起的10个工作日内通知备案单位予以纠正;发现定级不准的,应当在收到备案材料之日起的10个工作日内通知备案单位重新审核确定。运营、使用单位或者主管部门重新确定信息系统等级后,应当按照本办法向公安机关重新备案。

第十八条　受理备案的公安机关应当对第三级、第四级信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次,对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查,应当会同其主管部门进行。对第五级信息系统,应当由国家指定的专门部门进行检查。公安

机关、国家指定的专门部门应当对下列事项进行检查：

（一）信息系统安全需求是否发生变化，原定保护等级是否准确；

（二）运营、使用单位安全管理制度、措施的落实情况；

（三）运营、使用单位及其主管部门对信息系统安全状况的检查情况；

（四）系统安全等级测评是否符合要求；

（五）信息安全产品使用是否符合要求；

（六）信息系统安全整改情况；

（七）备案材料与运营、使用单位、信息系统的符合情况；

（八）其他应当进行监督检查的事项。

第十九条 信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，如实向公安机关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件：

（一）信息系统备案事项变更情况；

（二）安全组织、人员的变动情况；

（三）信息安全管理制度、措施变更情况；

（四）信息系统运行状况记录；

（五）运营、使用单位及主管部门定期对信息系统安全状况的检查记录；

（六）对信息系统开展等级测评的技术测评报告；

（七）信息安全产品使用的变更情况；

（八）信息安全事件应急预案，信息安全事件应急处置结果报告；

（九）信息系统安全建设、整改结果报告。

第二十条 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关管理规范和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求，按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。

第二十一条 第三级以上信息系统应当选择使用符合以下条件的信息安全产品：

（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或控股的，在中华人民共和国境内具有独立的法人资格；

（二）产品的核心技术、关键部件具有我国自主知识产权；

（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；

（四）产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；

（五）对国家安全、社会秩序、公共利益不构成危害；

（六）对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

第二十二条 第三级以上的信息系统应当选择符合下列条件的等级保护测评机构进行测评：

（一）在中华人民共和国境内注册成立（港澳台地区除外）；

（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

（三）从事相关检测评估工作两年以上，无违法记录；

（四）工作人员仅限于中国公民；

（五）法人及主要业务、技术人员无犯罪记录；

（六）使用的技术装备、设施应当符合本办法对信息安全产品的要求；

（七）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

（八）对国家安全、社会秩序、公共利益不构成威胁。

第二十三条　从事信息系统安全等级测评的机构，应当履行下列义务：

（一）遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；

（二）保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；

（三）对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

第四章　涉及国家秘密信息系统的分级保护管理

第二十四条　涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统的实际情况进行保护。非涉密信息系统不得处理国家秘密信息。

第二十五条　涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级。涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护管理办法和国家保密标准 BMB17—2006《涉及国家秘密的计算机信息系统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。保密工作部门和机构应当监督指导涉密信息系统建设使用单位准确、合理地进行系统定级。

第二十六条　涉密信息系统建设使用单位应当将涉密信息系统定级和建设使用情况及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。

第二十七条　涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。涉密信息系统建设使用单位应当依据涉密信息系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

第二十八条　涉密信息系统使用的信息安全保密产品原则上应当选用本国产品，并应当通过国家保密局授权的检测机构依据有关国家保密标准进行的检测，通过检测的产品由国家保密局审核发布目录。

第二十九条　涉密信息系统建设使用单位在系统工程实施结束后，应当向保密工作

部门提出申请，由国家保密局授权的系统测评机构依据国家保密标准 BMB22—2007《涉及国家秘密的计算机信息系统分级保护测评指南》，对涉密信息系统进行安全保密测评。涉密信息系统建设使用单位在系统投入使用前，应当按照《涉及国家秘密的信息系统审批管理规定》，向设区的市级以上保密工作部门申请进行系统审批，涉密信息系统通过审批后方可投入使用。已投入使用的涉密信息系统，其建设使用单位在按照分级保护要求完成系统整改后，应当向保密工作部门备案。

第三十条 涉密信息系统建设使用单位在申请系统审批或者备案时，应当提交以下材料：

（一）系统设计、实施方案及审查论证意见；

（二）系统承建单位资质证明材料；

（三）系统建设和工程监理情况报告；

（四）系统安全保密检测评估报告；

（五）系统安全保密组织机构和管理制度情况；

（六）其他有关材料。

第三十一条 涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密管理责任单位变更时，其建设使用单位应当及时向负责审批的保密工作部门报告。保密工作部门应当根据实际情况，决定是否对其重新进行测评和审批。

第三十二条 涉密信息系统建设使用单位应当依据国家保密标准 BMB20—2007《涉及国家秘密的信息系统分级保护管理规范》，加强涉密信息系统运行中的保密管理，定期进行风险评估，消除泄密隐患和漏洞。

第三十三条 国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督管理，并做好以下工作：

（一）指导、监督和检查分级保护工作的开展；

（二）指导涉密信息系统建设，使用单位规范信息定密，合理确定系统保护等级；

（三）参与涉密信息系统分级保护方案论证，指导建设使用单位做好保密设施的同步规划设计；

（四）依法对涉密信息系统集成资质单位进行监督管理；

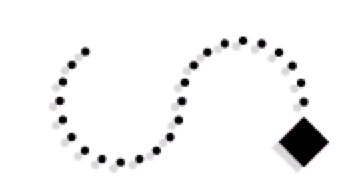
（五）严格进行系统测评和审批工作，监督检查涉密信息系统建设使用单位分级保护管理制度和技术措施的落实情况；

（六）加强涉密信息系统运行中的保密监督检查。对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评，对绝密级信息系统每年至少进行一次保密检查或者系统测评；

（七）了解掌握各级各类涉密信息系统的管理使用情况，及时发现和查处各种违规违法行为和泄密事件。

第五章　信息安全等级保护的密码管理

第三十四条 国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全



防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

第三十五条 信息系统安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。

第三十六条 信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

第三十七条 运用密码技术对信息系统进行系统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者对销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

第三十八条 信息系统中的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担，其他任何部门、单位和个人不得对密码进行评测和监控。

第三十九条 各级密码管理部门可以定期或者不定期对信息系统等级保护工作中的密码配备、使用和管理情况进行检查和测评，对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中，发现存在安全隐患或者违反密码管理相关规定或者未达到密码相关标准要求的，应当按照国家密码管理的相关规定进行处置。

第六章 法律责任

第四十条 第三级以上信息系统运营、使用单位违反本办法规定，有下列行为之一的，由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，并及时反馈处理结果：

（一）未按本办法规定备案、审批的；

（二）未按本办法规定落实安全管理制度、措施的；

（三）未按本办法规定开展系统安全状况检查的；

（四）未按本办法规定开展系统安全技术测评的；

（五）接到整改通知后，拒不整改的；

（六）未按本办法规定选择使用信息安全产品和测评机构的；

（七）未按本办法规定如实提供有关文件和证明材料的；

（八）违反保密管理规定的；

（九）违反密码管理规定的；

（十）违反本办法其他规定的。

违反前款规定，造成严重损害的，由相关部门依照有关法律、法规予以处理。

第四十一条　信息安全监管部门及其工作人员在履行监督管理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第七章　附　　则

第四十二条　已运行信息系统的运营、使用单位自本办法施行之日起180日内确定信息系统的安全保护等级；新建信息系统在设计、规划阶段确定安全保护等级。

第四十三条　本办法所称“以上”包含本数(级)。

第四十四条　本办法自发布之日起施行，《信息安全等级保护管理办法(试行)》(公通字[2006]7号)同时废止。

参 考 文 献

[1] 杨威.网络工程设计与安装[M].北京:电子工业出版社,2003.
[2] 王维江,钟小平.网络应用方案与实例精选[M].北京:人民邮电出版社,2003.
[3] 魏大新,李育龙.CISCO 网络技术教程[M].北京:电子工业出版社,2005.
[4] 杨卫东.网络系统集成与工程设计[M].北京:科学出版社,2005.
[5] 斯桃枝,李战国.计算机网络系统集成[M].北京:北京大学出版社,2006.
[6] 肖永生.网络互联技术[M].北京: 高等教育出版社,2006.
[7] 王淑江.精通 Windows Server 2008 活动目录与用户[M].北京:中国铁道出版社,2009.
[8] 肖德宝,徐慧.网络管理理论与技术[M].武汉:华中科技大学出版社,2009.
[9] 王达.Cisco/H3C 交换机配置与管理完全手册[M].北京:中国水利水电出版社,2009.
[10] 赵立群.计算机网络管理与安全[M].北京:清华大学出版社,2010.
[11] 王淑江.Windows Server 2008 R2 活动目录内幕[M].北京:电子工业出版社,2010.
[12] 王达.路由器配置与管理完全手册[M].武汉:华中科技大学出版社,2011.
[13] 刘晓晓.网络系统集成[M].北京:清华大学出版社,2012.

参考网站

[1] 百度文库. http://wenku. baidu. com.
[2] 游龙科技. http://www. siteview. com.
[3] 中国领先的 IT 技术网站. http://www. 51cto. com.
[4] 赛迪网. http://www. ccidnet. com.
[5] 搜狐. http://www. sohu. com.
[6] 百度. http://www. baidu. com.